NORMAN

SecuritySuite

Manuale dell'utente

versione 8.00

SAND BOX · STATISTICS · UPDATE · UNREAD MAIL · SECURED · VIRUS SCAN · DOCUMENTS

- Antivirus
- Antispam
- Intrusion Guard
- Personal Firewall
- Parental Control
- Privacy Tools

NORMAN®

Garanzia limitata

Norman garantisce che il CD-ROM o il DVD e la documentazione inclusi nella confezione non presentano difetti di produzione. Nel caso in cui si rilevi un difetto entro 30 giorni dalla data di acquisto, Norman sostituirà gratuitamente la documentazione e/o il CD-ROM o il DVD difettosi. Assieme ad ogni reclamo deve essere allegata una prova di acquisto del prodotto.

La presente garanzia è limitata alla sostituzione del prodotto. Norman non è responsabile di altre forme di perdita o danno risultanti dall'uso del software o della documentazione, né da relativi errori o difetti, incluso ma non limitatamente alla perdita di profitti.

Relativamente a difetti o anomalie del CD-ROM o del DVD, della documentazione o di questo accordo di licenza, la presente garanzia sostituisce ogni altra garanzia, esplicita o implicita, incluse, senza limitazioni, garanzie implicite di commerciabilità e idoneità per scopi particolari.

In particolare, e senza le limitazioni imposte dal contratto di licenza relativamente a qualsiasi uso o scopo specifico, Norman non sarà in alcun modo responsabile della perdita di profitti né di altri danni commerciali compresi, senza limitazioni, danni accidentali o indiretti.

La presente garanzia scade 30 giorni dopo la data di acquisto.

Le informazioni presenti in questo documento, così come la funzionalità del software, sono soggette a modifica senza preavviso. Il software può essere utilizzato secondo i termini del contratto di licenza. L'acquirente può eseguire una copia del software a scopo di backup. Nessuna parte di questa documentazione può essere riprodotta o trasmessa in alcuna forma e in alcun modo, elettronico o meccanico, comprese fotocopie, registrazione di informazioni e sistemi di recupero dati, per scopi diversi dall'uso personale dell'utente, senza espressa autorizzazione scritta di Norman.

Il logo Norman è un marchio registrato di Norman ASA.

I nomi dei prodotti citati in questo documento sono marchi di fabbrica o marchi registrati dei rispettivi proprietari e vengono citati esclusivamente a scopo di identificazione.

La documentazione e il software Norman sono protetti da:

Copyright © 1990-2010 Norman ASA.

Tutti i diritti riservati.

Revisione marzo 2010.

Introduzione 4
Requisiti di sistema 4
Informazioni sulla presente versione 4
Informazioni sul presente manuale 4
Addestramento e assistenza tecnica 4
Cos'è Norman Security Suite? 5
Antivirus & Antispyware 5
Personal Firewall 6
Antispam 7
Parental Control 7
Privacy Tools 7
Intrusion Guard 8

Installazione 9
Recupero del software 9
Chiave di licenza 10
Installazione 10
Procedure guidate 12
Installazione guidata 12

Introduzione 13
Icona della barra delle applicazioni 13
Icone di avviso della barra delle applicazioni 14
Apertura dell'applicazione 15
Icone di avviso del prodotto 15
Impostazioni di Security Suite 15

Pagina principale 16
Aggiornamento di tutti i prodotti 16
Attivazione/disattivazione degli aggiornamenti automatici 16

Antivirus & Antispyware 17
Pagina principale 17
Quarantena 18
Mantieni i file in quarantena 18
File in quarantena 19
Editor attività 19
Crea attività 20
Pianifica l'esecuzione delle scansioni 21
Elenco di esclusione 21
Impostazioni 22
Scanner automatico 23
Scanner manuale 25
Protezione Internet 26
Altri metodi di scansione 29

Personal Firewall 31
Pagina principale 31
Strumenti avanzati 33
Editor regole 33
Utility di log in tempo reale 36
Visualizzatore porte avanzato 37
Esporta regole Personal Firewall 38
Importa regole Personal Firewall 38
Impostazioni 39
Configura Personal Firewall 39
Impostazioni avanzate 39

Antispam 40
Pagina principale 40
Blocca/Consenti 42
Aggiunta/rimozione di indirizzi e-mail 42
Impostazioni 43
Configura livello filtro 43
Configura controllo spam 43

Parental Control 44
Pagina principale 45
Configurazione utente 46
Impostazioni predefinite del profilo 47
Crea utente 48
Visualizzatore log 50
Impostazioni 50

Privacy Tools 51
Eliminazione della cronologia dei programmi di un utente 51
Eliminazione sicura 52

Intrusion Guard 53
Pagina principale 53
Impostazioni 53
Driver e memoria 54
Processi 55
Rete 56

Installa e aggiorna 57
Pagina principale 57
Impostazioni 58
Seleziona metodo di aggiornamento 58
Impostazioni proxy 59

Centro di supporto 60
Pagina principale 60
Guida e risoluzione dei problemi 60
Informazioni di contatto 60
Riparazione automatica 61
Log dei messaggi 61

Disinstallazione di NSS 62

Appendice A 63
Sandbox 63

Appendice B 64
Advanced System Reporter 64
Elementi interni del sistema operativo 65
Internet Explorer 66
Processi 67

Copyright © 1990-2010 Norman ASA

Introduzione

Requisiti di sistema

Questa versione supporta l'installazione di Norman Security Suite v8.00 su computer con Windows XP, Windows Vista e Windows 7 in base alle seguenti specifiche:

Windows		XP	Vista	7
Antivirus		☑	☑	☑
Intrusion Guard		solo 32 bit	☑	☑
Personal Firewall			☑	☑
Parental Control			☑	☑
Antispam [1)]			☑	☑
Privacy Tools			☑	☑
Service Pack	o superiore	2	1	
CPU (basata su Pentium)	Consigliata	1,8 GHz		
RAM	Consigliata	2 GB		
Internet Explorer	o superiore	7 (8)		
Spazio su disco disponibile	Consigliato	500 MB		
Risoluzione schermo	Consigliata	1024x768		

[1)] L'applicazione Antispam può essere utilizzata solo con Windows Outlook, Outlook Express e Vista Mail.

Informazioni sulla presente versione

Questa versione è disponibile in diverse lingue. Di tanto in tanto vengono aggiunte nuove lingue. Rivolgersi al rappresentante Norman per avere informazioni su Security Suite nella lingua desiderata. Visitare i siti Web Norman per informazioni più dettagliate oppure rivolgersi al rappresentante locale per ulteriori informazioni sulle versioni disponibili nelle varie lingue.

Informazioni sul presente manuale

In questo manuale viene presentata una panoramica di prodotti, caratteristiche e funzioni chiave di Norman Security Suite. Fare riferimento alla Guida in linea per una spiegazione dettagliata di tutte le opzioni disponibili.

NOTA: note speciali o importanti sono contrassegnate con un punto esclamativo nel margine sinistro.

Addestramento e assistenza tecnica

Per l'addestramento o l'assistenza tecnica rivolgersi al rivenditore locale oppure a Norman ASA. Norman fornisce assistenza tecnica e servizi di consulenza per l'utilizzo di Security Suite e in generale per problematiche relative alla sicurezza. L'assistenza tecnica offre anche l'assicurazione della qualità dell'installazione dell'antivirus, compresa la consulenza per personalizzare Security Suite in base ad esigenze specifiche. La quantità di servizi disponibili può variare da paese a paese.

Informazioni di contatto per le sedi Norman sono disponibili nell'ultima pagina di questo documento.

Copyright © 1990-2010 Norman ASA

Cos'è Norman Security Suite?

Norman Security Suite (NSS) è un pacchetto software per la sicurezza costituito da sei diverse applicazioni:

☑ **Antivirus & Antispyware**	Blocca i virus impedendo di attaccare il computer
☑ **Personal Firewall**	Impedisce agli hacker di utilizzare il computer come mezzo per traffico indesiderato
☑ **Antispam**	Blocca messaggi e-mail non desiderati e di massa
☑ **Parental Control**	Impedisce ai bambini di accedere a siti Web con contenuto non desiderato
☑ **Privacy Tools**	Consente di eliminare in modo sicuro file e dati personali.
☑ **Intrusion Guard**	Impedisce a programmi dannosi di accedere al computer e infettarlo

* Le ultime due applicazioni, Privacy Tools e Intrusion Guard, sono incluse solo nella versione Security Suite PRO.

Per iniziare a utilizzare Norman Security Suite, è sufficiente installarlo. Le impostazioni di configurazione predefinite forniscono la protezione necessaria e non occorre modificare le opzioni di configurazione per rendere il programma operativo. Tuttavia, è utile conoscere il funzionamento di questo prodotto e familiarizzare con le relative funzioni di base. In questo manuale vengono descritte determinate funzioni utili e vengono forniti alcuni suggerimenti su come utilizzare al meglio il programma.

NOTA: è necessario eseguire una procedura guidata per iniziare a utilizzare Personal Firewall. Fare riferimento alla sezione "Installazione guidata" a pagina 12 per ulteriori informazioni.

Antivirus & Antispyware

Questo programma antivirus monitora il PC per rilevare eventuale software dannoso, chiamato anche malware. Per 'malware' si intendono virus, worm, cavalli di Troia e altri tipi di codice indesiderato.
I programmi spyware non sono distruttivi come i virus tradizionali, ma le conseguenze derivanti dalla divulgazione non volontaria di informazioni personali possono essere realmente dannose. La funzione univoca di Norman Sandbox offre una protezione proattiva che identifica anche virus sconosciuti.

Per ulteriori informazioni sulla funzione Sandbox di Norman, vedere pagina 63.

I virus possono essere automaticamente rimossi da dischi rigidi, unità rimuovibili, allegati e-mail, eccetera. L'applicazione Antivirus & Antispyware controlla i file al momento dell'accesso e rimuove automaticamente possibili virus. Security Suite prevede due scanner principali, lo scanner automatico e lo scanner manuale, nonché diversi metodi di scansione.

Poiché si consiglia agli utenti di eseguire scansioni manuali del computer, è possibile avviare una scansione dell'intero computer all'istante dalla barra delle applicazioni. È anche possibile avviare una scansione dal menu visualizzato facendo clic con il pulsante destro del mouse mentre si scorrono i file o scegliere lo screen saver di Norman che avvia una scansione quando attivato. Se si riprende il lavoro e la scansione viene interrotta, alla successiva attivazione dello screen saver, la scansione viene ripresa dal punto in cui è stata interrotta. Per scansioni manuali regolari, è possibile utilizzare l'utilità di pianificazione e l'editor attività per definire l'area del PC da sottoporre a scansione e gli orari in cui eseguire la scansione.

Questo prodotto viene fornito con impostazioni preselezionate in grado di proteggere in modo adeguato da attacchi di virus. I moduli possono essere configurati in base alle proprie esigenze.

Copyright © 1990-2010 Norman ASA

Personal Firewall

Ogni volta che si esegue un'operazione su Internet, ad esempio per leggere la posta elettronica o per navigare in rete, si stabilisce un collegamento con altri computer situati in varie parti del mondo. Da questo momento iniziano i problemi. Accedendo in modo non autorizzato al computer, gli hacker possono accedere a documenti privati, utilizzare il computer per azioni dannose e persino rendere il computer completamente inutilizzabile, cancellando importanti file di sistema.

Questa applicazione è la prima protezione da hacker e controlla il traffico in ingresso e in uscita del computer in base a criteri di sicurezza (gruppo di regole). Queste regole vengono stabilite (automaticamente o auto-definite) quando si installa il prodotto.

La procedura guidata per la creazione delle regole dell'applicazione può creare automaticamente le regole per gestire l'accesso delle applicazioni a Internet. Esistono diverse modalità per utenti esperti e inesperti e l'applicazione utilizza una tecnica di riconoscimento della "modalità server". È possibile creare e modificare regole e visualizzare dettagli su traffico e attività sulle porte.

Inoltre, l'applicazione avanzata Personal Firewall offre:

- **Protezione avvio**
  - Rileva i tentativi di un'applicazione di avviare se stessa tramite un'altra applicazione.
- **Protezione avvio furtivo**
  - Rileva applicazioni dannose che tentano di accedere a Internet tramite altre applicazioni. Personal Firewall tiene traccia di tutte le applicazioni principali.
- **Protezione deviazione processi**
  - Impedisce ad applicazioni dannose di deviare un processo "attendibile" per inserimento di .dll o thread.
- **Modalità nascosta completa**
  - Assicura che tutte le porte sul computer siano completamente invisibili dall'esterno.
- **Gestione avanzata svchost**
  - Dove ogni servizio svchost ha regole separate anziché una regola generale per proteggere il gruppo di servizi che ciascuna sessione Svchost.exe può contenere.
  - **Svchost** è un nome di processo host generico per servizi in Windows 2000/XP/2003/Vista che diversi processi di rete e Internet utilizzano per funzionare correttamente. Questo servizio può eseguire molte istanze completamente, ciascuna necessaria per il funzionamento del singolo computer. Il servizio ha una reale esigenza di accedere a Internet e, come qualsiasi altra applicazione in rete, il monitoraggio e la notifica di questo tipo di attività è di responsabilità del personal firewall. Sebbene molti firewall abbiano solo una regola generica per la gestione di processi svchost, spesso non modificabile, questo personal firewall distingue le diverse istanze e può stabilire se il processo è noto o sconosciuto. Inoltre, sono disponibili opzioni di configurazione per diversi servizi svchost nei file della Guida in linea dell'applicazione.
- **Anti-pharming**
  - Implementato mediante la protezione del file HOSTS e, quindi, eliminando il metodo di attacco pharming più comune.
  - Il termine **Pharming** è costruito con i termini "phishing" e "farming" (vedere la sezione Antispam di seguito per una spiegazione di "phishing"). Con "pharming" si intende quando un hacker tenta di reindirizzare il traffico dal sito Web che si sta visitando a un altro sito Web fittizio. Il pharming può essere eseguito modificando il file HOSTS sul computer di destinazione o sfruttando le vulnerabilità in software di server DNS. I server DNS (Domain Name Server) sono responsabili della risoluzione di nomi Internet in indirizzi reali. Negli ultimi anni, sia il "pharming" che il "phishing" sono stati utilizzati per furto di informazioni di identità online. Il "pharming" è diventato un problema più pressante per le aziende con host per e-commerce e siti Web di online banking. Misure sofisticate note come anti-pharming sono necessarie per proteggersi da questa importante minacce.

Copyright © 1990-2010 Norman ASA

Antispam

L'applicazione Antispam protegge da messaggi e-mail commerciali e di massa non richiesti (spam) che possono contenere minacce per il sistema. Antispam blocca spam, tentativi di phishing e altre minacce via e-mail prima che possano raggiungere il computer. È possibile creare elenchi di blocco e autorizzazione per gestire gli utenti da cui si ricevono messaggi e-mail e il contenuto trasmesso attraverso il proprio client e-mail.

Come le applicazioni antivirus sviluppano file di definizione dei virus per rilevare malware, le soluzioni antispam utilizzano file di definizione per filtrare messaggi e-mail non richiesti. I file di definizione dei virus contengono firme che determinano se un file è infetto o meno, mentre le definizioni antispam utilizzano una serie di criteri per determinare la probabilità che un messaggio e-mail sia un messaggio di spam. I file di definizione di spam basano l'analisi di un messaggio e-mail sulla lingua, sulle immagini, sui colori, sui collegamenti inclusi nel messaggio nonché sull'indirizzo e-mail e IP del mittente. Non è sempre possibile stabilire con assoluta certezza se un messaggio e-mail è spam.

- **Spam**
  - Posta elettronica non desiderata, solitamente pubblicità di qualche prodotto. I messaggi spam sono solitamente innocui, ma possono essere fastidiosi e una perdita di tempo.
- **Phishing**
  - L'atto di inviare un messaggio e-mail a un'altra persona presentandosi come una azienda pubblica o privata legittima nel tentativo di acquisire informazioni private che possono essere utilizzate per il furto di identità. Il messaggio e-mail indirizza l'utente in un sito Web dove viene richiesto di aggiornare informazioni personali, come il numero della carta di credito o del conto bancario, informazioni che l'organizzazione effettiva già possiede. Il sito Web è naturalmente falso, ma appare come organizzazione reale ed ha l'unico scopo di sottrarre informazioni. Il termine 'phishing' è una variazione del termine 'fishing', dove il gioco di parole è basato sul concetto di gettare l'amo con la speranza che qualcuno abbocchi.

Parental Control

Internet non è necessariamente un luogo ideale ed esistono molti siti Web che certamente non sono appropriati per i membri della famiglia più giovani. A meno che bambini e adolescenti non siano sotto il controllo di un adulto, è probabile che visitino siti Web con contenuti indesiderati, deliberatamente o meno.

Con Parental Control è possibile bloccare l'accesso a determinate categorie di siti Web o anche bloccare tutti i siti non esplicitamente approvati. Inoltre, è possibile limitare il tempo concesso a un utente per navigare in rete e specificare l'orario del giorno in cui l'utente è autorizzato a navigare.

In breve, è possibile personalizzare un profilo per il singolo utente in base all'età o ad altri criteri che si desidera tenere in considerazione.

Privacy Tools

Molte applicazioni, incluso il sistema operativo stesso, registrano l'attività dell'utente; ad esempio, l'apertura di file, l'accesso a siti Web o la visualizzazione di documenti. Si tratta di un utile meccanismo che consente agli utenti di eseguire attività ripetitive, come consultare il giornale online o continuare a lavorare su un documento di testo.

Sebbene sia utile, tale meccanismo può presentare problemi di privacy. Altri utenti del computer oppure persone che si trovino a ispezionare il computer in un secondo tempo potrebbero esaminare tali log e scoprire qualcosa che si desidera mantenere privato. Anche eliminando un file dal computer, questo non viene rimosso completamente. Strumenti avanzati sono in grado di recuperare il file compromettendo la sicurezza di documenti riservati. I log tengono traccia degli accessi a Internet e dell'apertura di file sul computer.

Questa funzionalità presenta problemi di privacy, in quanto rappresenta un potenziale rischio di ingegneria sociale e furto di identità o password. Le informazioni personali acquisite possono quindi essere utilizzate per scopi dolosi.

Copyright © 1990-2010 Norman ASA

Con Privacy Tools è possibile eliminare file specifici in modo sicuro. Il contenuto dei file viene cancellato in modo permanente e non può essere recuperato. È anche possibile configurare l'applicazione in modo che elimini automaticamente diversi file di log contenenti i dati personali, i cookie e la cronologia del browser. L'eliminazione di log della cronologia non ha effetti sulle impostazioni e sui segnalibri dell'applicazione.

Intrusion Guard

Questo è un sistema di prevenzioni intrusioni basato su host (HIPS), in grado di impedire ad applicazioni dannose di prendere il controllo del computer. L'applicazione offre un potente strumento di segnalazione degli errori e protegge processi, driver, browser e file HOSTS. È una piattaforma per la protezione proattiva da minacce destinata a utenti esperti.

- Advanced System Reporter
  - Questo potente strumento consente di controllare le applicazioni, i filtri di sistema e i moduli sospetti rilevati sul computer.
- Funzioni potenti in tempo reale
  - Questa funzione può essere configurata in modo da registrare, inviare un avviso e bloccare le intrusioni.
- Protezione processi
  - Impedisce ad applicazioni dannose di prendere il controllo di altre applicazioni e installare contenuto dannoso sul computer.
- Protezione driver
  - Impedisce l'installazione di driver e protegge da altre tecniche dannose che ottengono l'accesso a basso livello al sistema.
- Prevenzione del controllo del browser
  - Controlla le impostazioni di Internet Explorer e gestisce i cookie. Inoltre, è in grado di registrare, inviare avvisi e bloccare i tentativi di installazione dei filtri di rete, come LSP (Layered Service Provider) e BHO (Browser Helper Object).
- Protezione da file HOSTS
  - Protegge il file HOSTS da modifiche non autorizzate.

Copyright © 1990-2010 Norman ASA

Installazione

In questo capitolo vengono fornite informazioni sui requisiti di sistema, sulla chiave di licenza, sulla procedura di recupero del file di installazione e sull'installazione di Norman Security Suite sul computer.

Recupero del software

Al momento dell'acquisto di Norman Security Suite è stato fornito un CD con il file di installazione oppure nei documenti di acquisto è disponibile l'indirizzo di una pagina Web per scaricare il file da Internet.

CD-ROM

Se è stato fornito un CD-ROM da Norman, utilizzarlo per avviare l'installazione.

1. Inserire il CD nel lettore CD-ROM.
   - Il CD viene eseguito automaticamente e appare il menu del CD. Se il menu del CD non viene visualizzato entro un minuto circa, è possibile che la funzione per l'esecuzione automatica sia disattivata. Per avviare il menu del CD manualmente, effettuare quanto segue:
     - Sfogliare il contenuto del CD e fare doppio clic sul file principale Norman.exe.
     - Fare clic su **Start > Esegui** e immettere D:\Norman.exe. Sostituire D: con la lettera della partizione effettiva del proprio lettore CD-ROM. Fare clic su **OK**.
2. Scegliere la lingua per la visualizzazione del menu del CD.
3. Selezionare la lingua per l'installazione dalla pagina **Installa** del menu del CD.

Viene avviata la procedura guidata InstallShield. Continuare con la sezione "Installazione" a pagina 10.

Download da Internet

Il file di installazione può essere scaricato da Internet. La posizione Internet e la procedura di download sono incluse nelle informazioni dell'ordine di acquisto. In caso contrario, attenersi alle istruzioni seguenti per scaricare il file di installazione e avviare l'installazione.

1. Aprire il browser Internet e immettere l'indirizzo Web generale per i download software di Norman: **http://www.norman.com/downloads/**
2. Selezionare il file di installazione di Norman Security Suite in base alla lingua e/o alla versione.

NOTA: scegliere il file di installazione corretto in base al computer, 64 o 32 bit.

3. Fare clic su **Salva** o **Esegui**.

   a) **Salva**
   Se si fa clic su **Salva** è possibile salvare il file sul computer e avviare l'installazione da questa posizione. Quando si esegue l'installazione dal computer non occorre una connessione Internet. Tuttavia, si consiglia di utilizzare una connessione Internet durante l'installazione per la convalida della chiave e l'aggiornamento.
   - Individuare una cartella in cui salvare il file di installazione e fare clic su **Salva** per confermare.
     - Prendere nota della posizione in cui si salva il file di installazione.
     - Come la finestra del download, anche il browser non è più necessario e può essere chiuso.
   - Individuare il file di installazione e fare doppio clic sul file.
     - Il file di installazione può essere eliminato una volta eseguita correttamente l'installazione o salvato su un supporto esterno per backup.

   b) **Esegui**
   Fare clic su **Esegui** per avviare l'installazione direttamente da Web. Il file di installazione viene scaricato e viene avviata immediatamente l'installazione del prodotto. Se si verifica un problema di installazione, visitare nuovamente la pagina per il download.

Viene attivata la procedura guidata InstallShield. Continuare con la sezione "Installazione" a pagina 10.

Copyright © 1990-2010 Norman ASA

Chiave di licenza

Quando si acquista Norman Security Suite si riceve una chiave di licenza del prodotto. La chiave è necessaria per l'aggiornamento dell'installazione. Un software antivirus non aggiornato regolarmente non è efficiente.

Chiave disponibile

Immettere la chiave durante l'installazione, quando richiesto dalla procedura guidata InstallShield. L'applicazione ricerca automaticamente gli aggiornamenti non appena viene terminata l'installazione.

Chiave non disponibile

È possibile lasciare vuoto il campo della chiave e installare comunque l'intera suite. Tuttavia, in tal caso, la funzionalità Gestione licenza guidata continuerà a richiedere regolarmente una chiave e i prodotti non verranno aggiornati.

Immissione di una chiave una volta terminata l'installazione

È possibile attivare la procedura Gestione licenza guidata dall'applicazione e incollare la chiave nel campo appropriato. Fare riferimento alla sezione "Gestione licenza guidata" a pagina 58.

Installazione

Eseguire la procedura guidata InstallShield di Norman Security Suite (file di installazione). Fare riferimento alla sezione "Recupero del software" a pagina 9 per informazioni su come ottenere il software. Seguire le istruzioni visualizzate sullo schermo. Fare clic su **Indietro** se occorre rivedere o modificare le impostazioni di installazione.

La posizione predefinita per l'installazione è `C:\Programmi\Norman`**.**

1. Viene visualizzata la schermata iniziale della procedura guidata InstallShield. Fare clic su **Avanti**.
2. Leggere il contratto di licenza e accettarlo per continuare l'installazione. Fare clic su **Avanti**.
3. Immettere una chiave di licenza del prodotto valida. Fare clic su **Avanti**.
   - La chiave contiene informazioni sui prodotti acquistati.
   - È possibile lasciare vuoto il campo se si desidera solo valutare il prodotto. Si consiglia di immettere una chiave di prova per eseguire il maggior numero di operazioni con il prodotto durante il periodo di prova.

SUGGERIMENTO

COPIARE E INCOLLARE LA CHIAVE DI LICENZA. Se si dispone di una copia della chiave di licenza in un messaggio e-mail o in un altro formato elettronico, il modo più facile è copiare la chiave nell'apposito campo. Evidenziare la chiave e premere **Ctrl+C**, posizionare il cursore nel campo della chiave di licenza e premere **Ctrl+V** per incollare la chiave. Accertarsi che non vengano inclusi spazi.

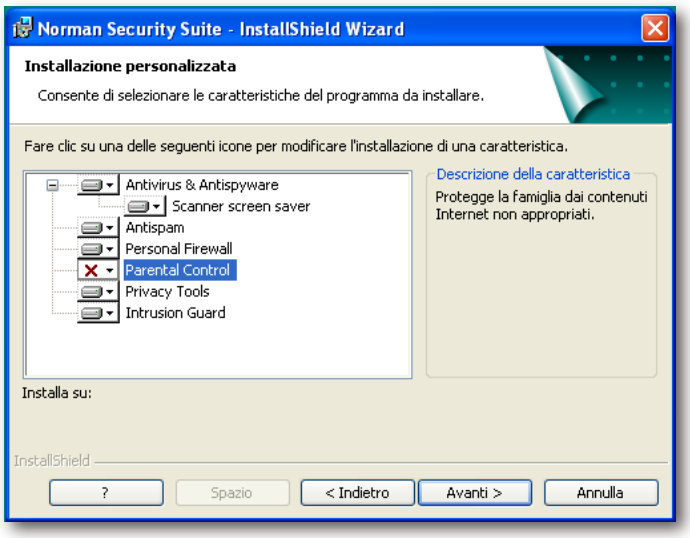
NOTA: se non si dispone di una chiave, è possibile lasciare vuoto il campo e installare comunque l'intera suite. Tuttavia, in tal caso, la funzionalità Gestione licenza guidata continuerà a richiedere regolarmente una chiave e i prodotti non verranno aggiornati. Se necessario, la funzionalità Gestione licenza guidata fornirà le informazioni necessarie per ottenere una chiave in un secondo momento.

4. **Tipo di installazione**
   a) Selezionare **Completa** per installare tutte le funzionalità del programma nella posizione predefinita.
      - Selezionare **Completa** e fare clic su **Avanti**.
      - Continuare con il punto “7. Pronto per installazione” di seguito.

   b) Selezionare **Personalizzata** per decidere i prodotti da installare e/o selezionare un'altra posizione diversa dalla posizione predefinita.
      - Selezionare **Personalizzata** e fare clic su **Avanti**.
5. **Installazione personalizzata**
   Viene visualizzato un elenco di prodotti che è possibile installare.
   - **Antivirus & Antispyware**
     - **Scanner screen saver**

Copyright © 1990-2010 Norman ASA

- **Antispam**
- **Personal Firewall**
- **Parental Control**
  - Selezionare manualmente il prodotto che si desidera installare. Fare clic sul menu a discesa a sinistra e selezionare per installare la funzione sul disco rigido locale. L'installazione richiede che questo prodotto sia incluso nella chiave di licenza o faccia parte di un'installazione di prova.
  - Se si desidera, è anche possibile installare il prodotto successivamente.
- **Privacy Tools**
- **Intrusion Guard**



- Fare clic su **Spazio** se si desidera visualizzare lo spazio su disco richiesto per installare le funzionalità selezionate.
  - Fare clic su **OK** per tornare alla schermata **Installazione personalizzata**.
- Fare clic su **Avanti** per continuare.

6. **Cartella di destinazione**

   a) Fare clic su **Avanti** se si desidera installare le applicazioni selezionate nella posizione predefinita.

   b) Fare clic su **Cambia...** per definire un'altra posizione.
   - Selezionare la posizione dall'elenco a discesa, aggiungere una nuova cartella o immettere il percorso nel campo di input del nome della cartella.
   - Fare clic su **OK** per confermare e tornare alla schermata della cartella di destinazione.
   - Fare clic su **Avanti**.

7. Pronto per installazione
   - Fare clic su **Installa** per avviare l'installazione.
8. Installazione di Norman Security Suite
   - Viene visualizzata una finestra di dialogo per indicare che l'applicazione è pronta per avviare e configurare i componenti installati. Fare clic su **OK** per continuare.
9. Viene visualizzata la finestra di dialogo finale. Fare clic su **Fine** per completare la procedura guidata **InstallShield**. L'installazione continuerà in background per 5-10 minuti.
10. Fare clic su **Riavvia ora** quando viene richiesto di riavviare il computer. Una volta riavviato il computer, viene visualizzato un modulo di registrazione per il cliente e, se è installato Personal Firewall, la procedura guidata per l'installazione di Personal Firewall.
    - **Informazioni sul cliente**
      - Immettere le informazioni richieste e fare clic su **Invia**.
    - **Installazione guidata**
      - Fare riferimento alla sezione seguente.

Copyright © 1990-2010 Norman ASA

Procedure guidate

Norman Security Suite prevede tre diverse procedure guidate. Tali procedure gestiscono l'installazione e le configurazioni di base dei prodotti.

Procedura guidata InstallShield
Questa procedura guidata consente di installare Norman Security Suite. È anche nota come file di installazione.

Installazione guidata
Tale procedura viene utilizzata quando è installato Personal Firewall. Una volta installato Norman Security Suite con Personal Firewall, viene avviata una procedura guidata per la configurazione del Personal Firewall. Fare riferimento alla sezione seguente.

Gestione licenza guidata
Questa procedura guidata tiene traccia delle licenze di prodotti valide. Fare riferimento alla sezione "Gestione licenza guidata" a pagina 58.

Installazione guidata

È stata completata l'installazione di Norman Security Suite (vedere "Installazione" a pagina 10) e Personal Firewall è una delle funzionalità installate. Viene avviata automaticamente l'Installazione guidata.

Questa procedura guidata stabilisce alcune regole di base automaticamente, ad esempio concedendo alle applicazioni appropriate l'accesso a Internet. Lo scopo della procedura è identificare i programmi con una reale esigenza di accedere a Internet e creare regole per queste applicazioni. È altamente consigliato eseguire la procedura di installazione guidata. È possibile sempre modificare le regole generate automaticamente in un secondo momento, utilizzando l'Editor regole.

Se si sceglie di non eseguire l'Installazione guidata, è possibile che il computer non possa connettersi a Internet e che applicazioni importanti non vengano aggiornate. Fare riferimento alla sezione "Strumenti avanzati" a pagina 33.

1. Leggere la pagina dell'introduzione e fare clic su **Avanti**.
   L'Installazione guidata prevede operazioni diverse per utenti esperti e utenti inesperti. L'utente esperto può specificare determinati dettagli, mentre l'utente inesperto è guidato dalle configurazioni automatiche.
2. Valutare il proprio livello di esperienza e fare clic su **Avanti**.

   Utente inesperto
   - Utente di Internet standard senza esperienza o interesse specifico per l'aspetto tecnico dei computer. Il firewall prenderà automaticamente le decisioni e limiterà al minimo l'interazione dell'utente con il programma.
   - Selezionare il livello di sicurezza per la gestione delle connessioni Internet che tentano di accedere al computer (in ingresso) o applicazioni che tentano di connettersi a Internet (in uscita).
     - **Modalità Base**
       - È consentito tutto il traffico, a meno che una regola permanente non impedisca la connessione. Il computer sarà protetto da attacchi in entrata.
     - **Modalità Normale**
       - Viene richiesto di consentire o rifiutare traffico sconosciuto, a meno che una regola permanente non impedisca la connessione. Il computer sarà protetto da attacchi in entrata e applicazioni indesiderate che inviano dati dal computer.

   Utente esperto
   - Utente che conosce le operazioni di installazione del firewall standard ed è in grado di identificare indirizzo e numero di porta IP. Il firewall offre più opzioni avanzate durante l'installazione e l'uso.
3. Seguire le istruzioni visualizzate sullo schermo per aggiungere altri browser Web o client e-mail, configurare risorse di rete (configurazione avanzata, se l'utente è esperto) e consentire altre applicazioni note.
4. Infine, fare clic su **Fine** per completare la procedura guidata.

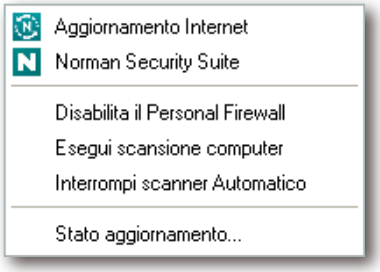
Copyright © 1990-2010 Norman ASA

Introduzione

Icona della barra delle applicazioni

Durante l'installazione viene inserita un"icona nella barra delle applicazioni, nell'angolo in basso a destra dello schermo. Questa icona conferma che Security Suite è installato su questo computer.

Fare clic con il pulsante destro del mouse sull'icona della barra delle applicazioni per visualizzare il menu della barra delle applicazioni Security Suite.



Le voci dell'elenco precedute da un'icona sono una copia delle opzioni presenti nel menu **Start > Programmi > Norman Security Suite**. Si tratta di un menu di scelta rapida che consente di accedere ai moduli principali di Norman Security Suite e ad alcune operazioni tipiche.

- **Aggiornamento Internet**
  - Consente di attivare la funzione Aggiornamento Internet e aggiornare i prodotti installati.
- **Norman Security Suite**
  - Consente di aprire l'applicazione Norman Security Suite.
- **Disabilita il Personal Firewall (Abilita il Personal Firewall)**
  - Consente di abilitare o disabilitare il Personal Firewall.
- **Esegui scansione computer**
  - Consente di avviare una scansione manuale dell'intero computer.
- **Interrompi scanner Automatico (Avvia scanner Automatico)**
  - Consente di avviare e arrestare lo scanner automatico.
- **Stato aggiornamento...**
  - Consente di visualizzare lo stato dell'aggiornamento per i prodotti installati. Inoltre, questa funzione consente di visualizzare messaggi relativi ai file di definizione dei virus scaduti, alla scadenza della licenza e altre informazioni.

NOTA: le opzioni del menu variano in base ai prodotti installati. Ad esempio, l'opzione per abilitare o disabilitare il Personal Firewall è visibile solo quando è installato il Personal Firewall.

Copyright © 1990-2010 Norman ASA

Icone di avviso della barra delle applicazioni

L'icona della barra delle applicazioni fornisce anche informazioni sullo stato dell'installazione di Security Suite. Posizionare il cursore sull'icona per una spiegazione di eventuali errori o messaggi.

Cerchio rosso

Questa icona indica che alcuni componenti attualmente in esecuzione non sono aggiornati. Se l'icona appare con il simbolo rosso lampeggiante, posizionare il mouse sul simbolo per controllare il componente che deve essere aggiornato o se si sono verificati altri errori.

NOTA: il simbolo rosso è visibile all'avvio fino a quando non sono stati avviati tutti i moduli. Più è lenta la macchina, più tempo occorre per caricare tutti i moduli. Tuttavia, l'icona Norman standard viene visualizzata dopo un massimo di due minuti.

Triangolo giallo

L'icona del triangolo giallo, fissa o lampeggiante, indica che lo scanner automatico è stato disabilitato manualmente, l'applicazione è in attesa di un riavvio, si è verificato un errore di installazione o i file di definizione non sono aggiornati.

- **Fissa**
  - Lo scanner automatico è stato disabilitato manualmente nelle impostazioni dell'applicazione. Fare riferimento alla sezione "Abilita scanner automatico" a pagina 23.
  - L'applicazione è in attesa di un riavvio. È possibile che l'opzione **Riavvia poi** sia stata selezionata in una richiesta precedente.
  - Si è verificato un possibile errore di installazione. Provare a riavviare il computer per risolvere l'errore.

- **Lampeggiante**
  - I file di definizione dei virus non sono aggiornati. Ciò significa che non sono stati aggiornati da oltre 10 giorni.
  - Lo scanner automatico è stato arrestato dal menu della barra delle applicazioni. Fare clic con il pulsante destro del mouse sull'icona della barra delle applicazioni. Selezionare **Avvia scanner Automatico**.
  - Il firewall è stato disabilitato. Fare clic con il pulsante destro del mouse sull'icona della barra delle applicazioni. Selezionare **Abilita il Personal Firewall**.

Ruota dentata gialla

Quando viene visualizzata l'icona con una ruota dentata, Norman Program Manager sta utilizzando il programma, probabilmente per un aggiornamento. Si consiglia di non spegnere il computer quando è in esecuzione NPM, ossia quando viene visualizzato questo simbolo.

NOTA: un aggiornamento non richiede più di 5-10 minuti. Se l'icona con la ruota dentata rimane visualizzata per un periodo di tempo più lungo, è possibile che si sia verificato un problema di installazione. In tal caso, provare a riavviare il computer. Se l'icona rimane ancora visualizzata, provare a utilizzare l'opzione di riparazione descritta nella sezione "Riparazione automatica" a pagina 61.

Simbolo di Windows Security Center

Norman è uno dei fornitori di antivirus rilevati dal sistema operativo. Se i file di definizione dei virus non sono aggiornati, lo scanner automatico non è in esecuzione o il firewall è disabilitato, Windows visualizza un avviso per indicare che si è verificato un errore. Viene visualizzato il simbolo del Security Center ed è possibile fare clic su di esso per visualizzare e modificare le impostazioni di Windows.

Copyright © 1990-2010 Norman ASA

Apertura dell'applicazione

È possibile aprire l'applicazione mediante il menu della barra delle applicazioni o mediante il menu Windows. Fare clic con il pulsante destro del mouse sull'icona della barra delle applicazioni del programma e selezionare **Norman Security Suite** dal menu popup. Dal menu Windows, fare clic su **Start** e selezionare **Programmi > Norman Security Suite > Norman Security Suite**.

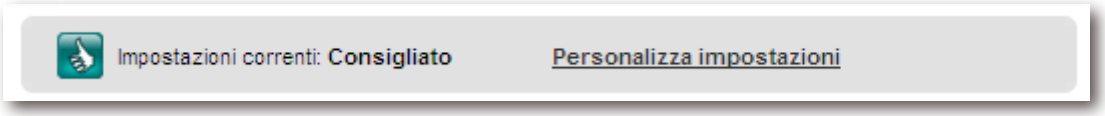
Icone di avviso del prodotto

A volte, appare un triangolo giallo sulla voce di menu dell'applicazione. In questo caso, è possibile che il prodotto sia disabilitato o non aggiornato, la licenza sia scaduta, un software installato recentemente richieda una configurazione finale per terminare la procedura di installazione e così via. Selezionare la voce di menu con l'avviso per ulteriori informazioni.

NOTA: quando si apre Security Suite per la prima volta, viene visualizzato un avviso per l'applicazione Parental Control. Fare riferimento alla sezione "Parental Control" a pagina 44.

Impostazioni di Security Suite

Questa applicazione è installata con impostazioni predefinite che si consiglia di utilizzare per l'esecuzione di attività quotidiane. È possibile selezionare **Personalizza impostazioni** dalle pagine principali dell'applicazione per configurare i prodotti attraverso diverse opzioni. Quando si modifica un'impostazione, notare la modifica dell'icona e della posizione del testo.



- Impostazioni correnti: **Consigliato**
  - Sono attive le impostazioni predefinite, consigliate per attività quotidiane.
  - Fare clic su **Personalizza impostazioni** se si desidera modificare le impostazioni predefinite.

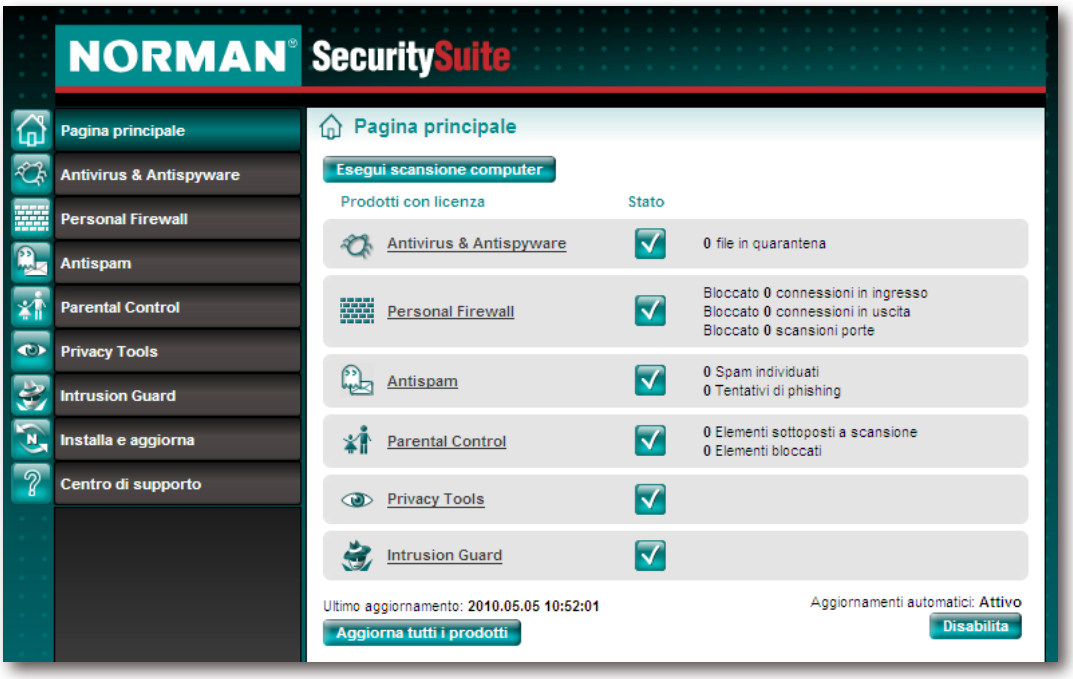
- Impostazioni correnti: **Personalizza**
  - Le impostazioni predefinite sono o possono essere personalizzate.
  - Fare clic su **Usa impostazioni consigliate** per ripristinare i valori predefiniti.

NOTA: non è consigliabile modificare le impostazioni predefinite, a meno che non si conosca l'effetto delle modifiche sul sistema. Accertarsi che le impostazioni personalizzate non determinino un livello di sicurezza inferiore. In caso di dubbio, tenere presente che le impostazioni predefinite garantiscono una protezione sufficiente.

Copyright © 1990-2010 Norman ASA

Pagina principale

Aprire l'applicazione Security Suite per visualizzare lo stato dei prodotti installati. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione.



Eseguire la scansione del computer, tenere traccia dei prodotti installati e del relativo stato e visualizzare informazioni dettagliate sui prodotti. Aggiornare tutti i prodotti e attivare o disattivare gli aggiornamenti automatici con un solo clic.

Fare clic su **Esegui scansione computer** per avviare una scansione manuale dell'intero computer. Questa scansione utilizza le stesse impostazioni come specificato per lo scanner Manuale. Vedere la sezione "Scanner manuale" a pagina 25.

I **prodotti con licenza** sono i prodotti coperti dalla chiave di licenza. Fare riferimento alla sezione "Chiave di licenza" a pagina 10. L'icona dello stato indica se l'installazione è aggiornata e completa, se occorre un aggiornamento o se il prodotto non è installato. Le statistiche a destra visualizzano i dati delle applicazioni in uso.

NOTA: quando si apre Security Suite per la prima volta, viene visualizzato un avviso per l'applicazione Parental Control. Fare riferimento alla sezione "Parental Control" a pagina 44.

Aggiornamento di tutti i prodotti

È possibile aggiornare tutti i prodotti installati con un semplice clic. Per ulteriori impostazioni e una panoramica, fare riferimento alla sezione "Installa e aggiorna" a pagina 57.

Attivazione/disattivazione degli aggiornamenti automatici

I prodotti verranno aggiornati regolarmente quando gli aggiornamenti automatici sono attivi. Modificare le impostazioni come descritto nella sezione "Seleziona metodo di aggiornamento" a pagina 58.

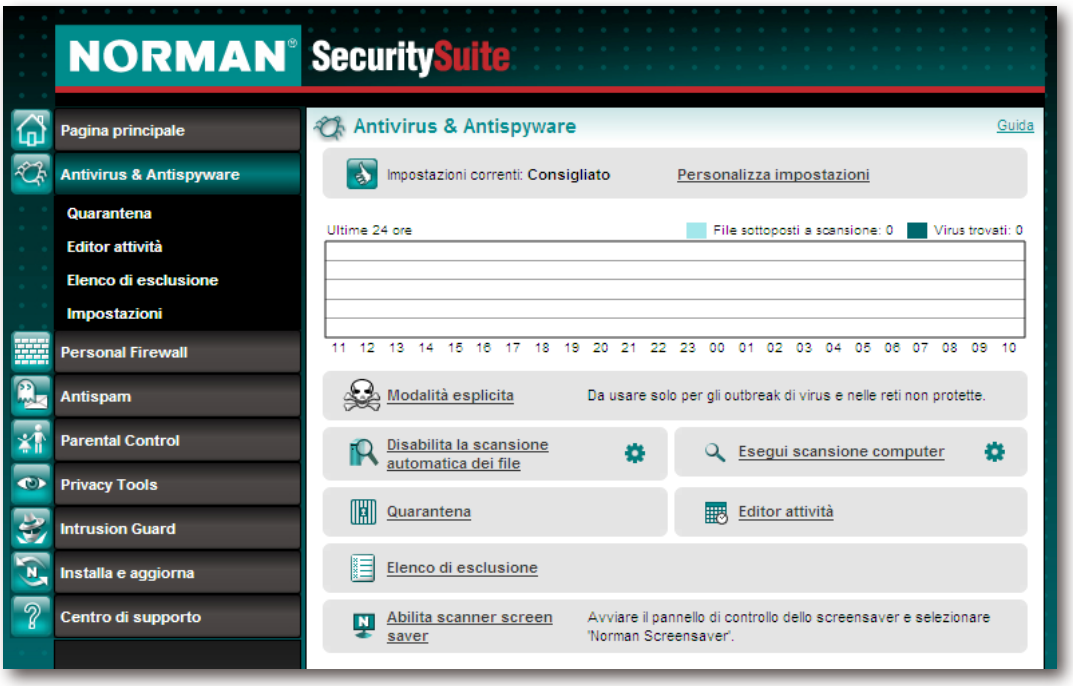
NOTA: è altamente consigliato attivare sempre gli aggiornamenti automatici.

Copyright © 1990-2010 Norman ASA

Antivirus & Antispyware

Aprire l'applicazione Security Suite e selezionare **Antivirus & Antispyware** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione e alla sezione "Antivirus & Antispyware" a pagina 5 per una descrizione dello scopo e della funzione dell'applicazione.

Pagina principale



L'applicazione Antivirus & Antispyware monitora il proprio computer per rilevare eventuale software dannoso, chiamato anche malware. In questo capitolo viene descritto come configurare i due principali scanner di virus, lo scanner automatico e lo scanner manuale, e come gestire file in quarantena, pianificare scansioni, attivare lo scanner screen saver e abilitare la funzionalità antispyware.

Personalizza impostazioni

Fare clic su questa opzione per modificare i valori predefiniti. Fare riferimento alla sezione "Impostazioni" a pagina 22. Per informazioni generali sulla selezione delle impostazioni consigliate o personalizzate, fare riferimento alla sezione "Impostazioni di Security Suite" a pagina 15.

Statistiche di scansione

La pagina principale dell'applicazione visualizza una rappresentazione grafica dei file analizzati e identificati come infetti nelle ultime 24 ore. Le statistiche riflettono l'attività combinata dello scanner manuale e dello scanner automatico.

Modalità esplicita

Si consiglia di attivare temporaneamente questa funzione solo in caso di outbreak di virus e nel collegamento a reti wireless sconosciute o non protette. L'abilitazione di questa opzione può incidere su prestazioni e stabilità.

Disabilita la scansione automatica dei file

Fare riferimento alla sezione **Impostazioni > Scanner automatico a** pagina 23.

Copyright © 1990-2010 Norman ASA

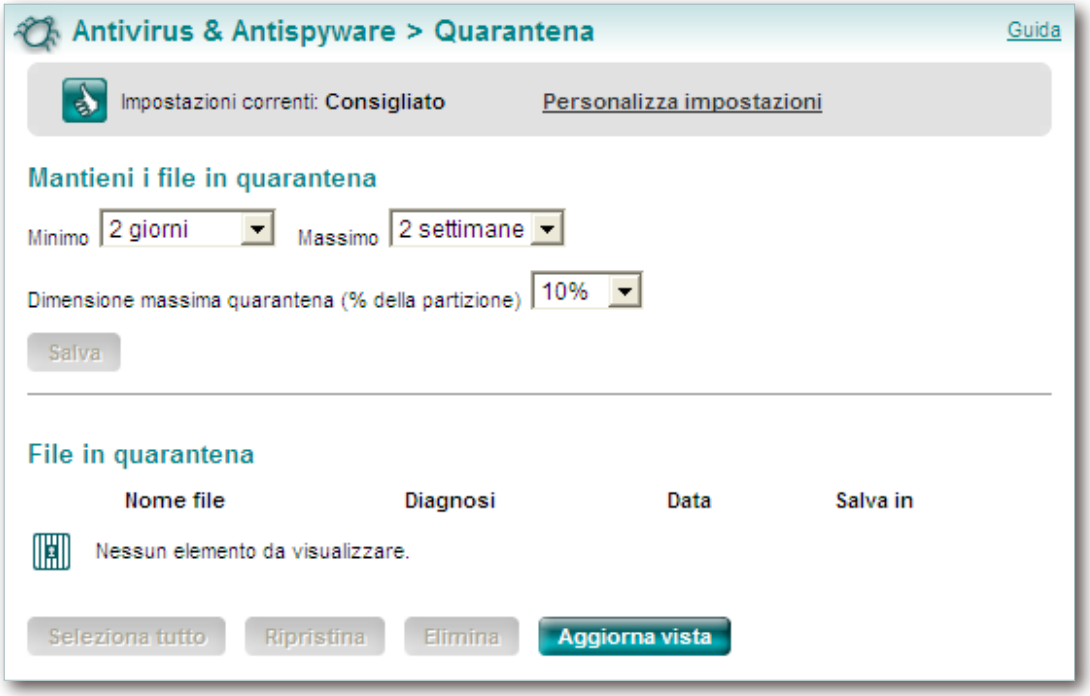
Esegui scansione computer

In questo caso, lo scanner manuale avvia una scansione di tutti i dischi rigidi del sistema. Dalla finestra di dialogo di scansione visualizzata è possibile selezionare **Interrompi** se si desidera **ricercare** un'altra posizione da sottoporre a scansione. Fare clic su **Avvia** per continuare la scansione manuale.

È anche possibile avviare questa scansione dal menu della barra delle applicazioni. Fare clic con il pulsante destro del mouse sull'icona della barra delle applicazioni e selezionare **Esegui scansione computer**.

Fare riferimento alla sezione "Scanner manuale" a pagina 25 per informazioni su come configurare lo scanner manuale.

Quarantena



Mantieni i file in quarantena

Selezionare **Personalizza impostazioni** per accedere alle opzioni di configurazione. Specificare il tempo minimo e massimo della quarantena e quanto spazio su disco è consentito utilizzare.

- **Minimo**
  Specificare un periodo compreso tra un giorno e una settimana. Questa opzione gestisce la permanenza minima dei file in quarantena.
- **Massimo**
  Specificare un periodo compreso tra una e quattro settimane. I file che superano il tempo massimo di permanenza in quarantena vengono eliminati senza preavviso.
- **Dimensione massima quarantena (% della partizione)**
  Specificare la quantità di spazio su disco della partizione corrente che i file in quarantena possono occupare.

NOTA: la dimensione massima consentita può essere superata nel caso in cui i file in quarantena non abbiano ancora raggiunto il tempo minimo specificato.

- Fare clic su **Salva** per confermare le modifiche.

Copyright © 1990-2010 Norman ASA

File in quarantena

I file infetti messi in quarantena vengono visualizzati nell'elenco **File in quarantena**, se il programma è stato configurato per eseguire questa operazione. L'applicazione antivirus proverà a pulire i file infetti prima di eliminarli o metterli in quarantena (in base alla configurazione). I file in quarantena sono infetti o sono stati bloccati dalla funzione Protezione Internet.

NOTA: per impostazione predefinita, una copia del file eliminato o bloccato viene messa in quarantena.

Una copia di un file infetto o messo in quarantena viene eliminata, se risiede in un'altra cartella viene spostata in quarantena. Quando lo scanner automatico rileva che il file `C:\eicar.com` è infetto, lo sposta in quarantena. Tuttavia, se lo scanner automatico rileva il file `C:\Copia di eicar.com` e tale file è identico a `eicar.com`, il file rilevato non viene messo in quarantena, ma eliminato. Se il file `Copia di eicar.com` risiede in `C:\altra cartella\`, viene spostato in quarantena perché in una nuova posizione. Questo metodo viene adottato per evitare un numero troppo elevato di file in quarantena nel caso in cui un virus abbia scritto diverse copie dello stesso file nella stessa area dell'unità disco rigido.

Un file può essere messo in quarantena perché l'applicazione Antivirus sospetta che sia infetto. In rare occasioni e in seguito all'aggiornamento dei file delle definizioni, è possibile che l'applicazione Antivirus determini che un file precedentemente messo in quarantena sia in effetti pulito. Poiché i tipi e le tecniche per la creazione e il rilevamento dei virus cambiano rapidamente, l'applicazione Antivirus sottopone a scansione la quarantena in seguito a un aggiornamento o a un riavvio del computer.

Se dopo tale controllo, un file in quarantena viene giudicato 'non pericoloso', verrà ripristinato a condizione che esista un percorso valido e che non sia già presente un file con lo stesso nome. Non è richiesto alcun intervento da parte dell'utente e non si verrà informati di un possibile ripristino di un file in quarantena.

Editor attività

A volte è pratico definire delle operazioni che devono essere eseguite più volte e/o a intervalli regolari. La ricerca di virus è un buon esempio di un'operazione che deve essere eseguita regolarmente e l'Editor attività è lo strumento fornito a questo scopo.

È possibile creare un file di attività per le scansioni che vengono eseguite ripetutamente o speciali scansioni che si desidera eseguire in determinate situazioni. Ad esempio, se si scaricano file da Internet in aree specifiche, è possibile creare un file di attività che esegua la scansione di tali aree ed esegua l'attività manualmente dopo il download. Inoltre, è possibile pianificare l'attività in modo che venga eseguita a un'ora prestabilita.

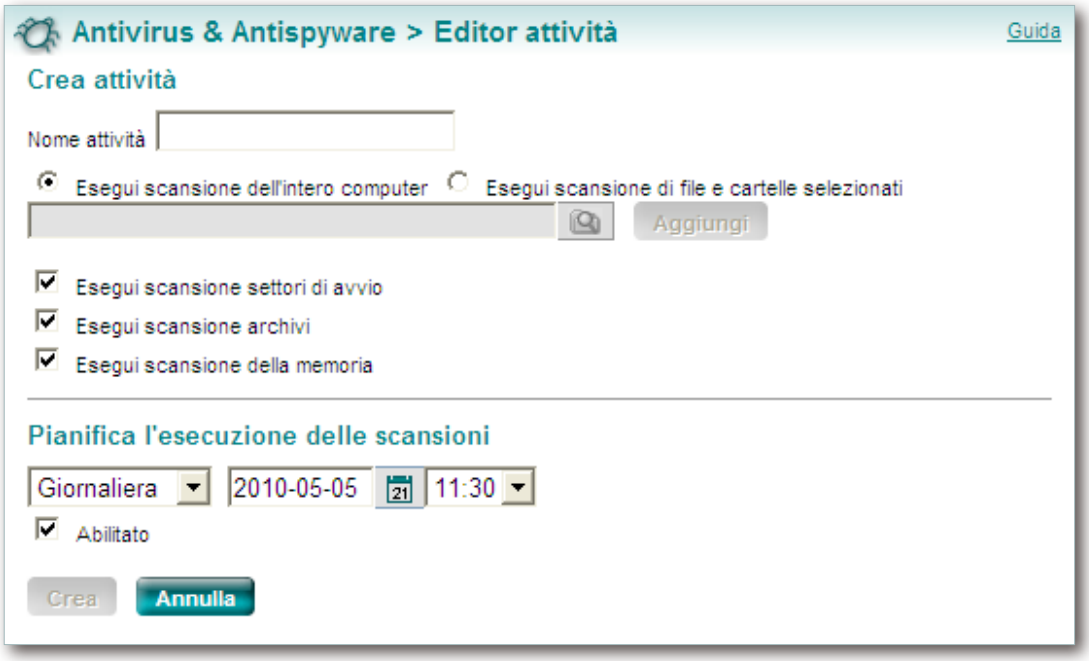
Gli amministratori possono creare dei file delle attività e distribuirli a tutte le workstation in rete per garantire che le aree che richiedono un'attenzione particolare vengano controllate regolarmente.

NOTA: la finestra di dialogo Crea attività appare la prima volta che si accede all'Editor attività oppure se non è stata creata ancora alcuna attività.

Tutte le attività esistenti vengono visualizzate in un elenco nella finestra di dialogo Editor attività.

Copyright © 1990-2010 Norman ASA

Crea attività



1. Immettere un **Nome attività**.
2. Selezionare **Esegui scansione dell'intero computer** o **Esegui scansione di file e cartelle selezionati**.
   - Fare clic sul simbolo di ricerca della cartella per visualizzare i file o le cartelle.
     - Nella parte inferiore della schermata vengono elencate tutte le unità locali. La schermata funziona in modo analogo a Esplora risorse di Windows.
     - Per visualizzare le directory o i file presenti nell'unità, fare clic su una lettera di unità.
     - Se si selezionano file e cartelle specifici, tutte le sottocartelle delle unità o delle cartelle selezionate verranno a loro volta selezionate automaticamente. È possibile deselezionare le sottocartelle che non si desidera includere nella scansione.
   - È anche possibile immettere un percorso e un nome file o directory nel campo di testo di input.
     - Il carattere jolly asterisco (*) è supportato. Ad esempio C:*.* indica la scansione dell'intera unità C.
     - Posizionare il carattere jolly all'inizio o alla fine del termine da ricercare. Non posizionare il carattere jolly al centro del termine da ricercare.
   - Quando si fa clic su **Aggiungi** per salvare, l'area specificata viene aggiunta all'elenco delle attività.
3. Selezionare una o più opzioni di scansione. **Esegui scansione settori di avvio**, **Esegui scansione archivi** ed **Esegui scansione della memoria** sono tutte opzioni preselezionate. Oltre a tale opzioni, vengono utilizzate le opzioni di scansione dello scanner manuale.
   - **Esegui scansione settori di avvio**
     - Quando si seleziona questa opzione, viene verificato il settore di avvio delle aree sottoposte a scansione.
   - **Esegui scansione archivi**
     - Selezionare questa opzione per includere nella scansione i file archivio (file compressi). Attualmente sono supportati i seguenti formati: ACE, APPLE_SINGLE, ARJ, BZIP2, CAB, GZ, LZH, MAIL, RAR, RAR3, SFXZIP, TAR, ZIP e 7Z.
   - **Esegui scansione della memoria**
     - Quando si esegue la scansione della memoria, vengono ricercati eventuali virus residenti nella memoria. È sempre opportuno verificare che la memoria sia libera da virus.

Copyright © 1990-2010 Norman ASA

Pianifica l'esecuzione delle scansioni

4. Selezionare frequenza, ora e data per l'esecuzione della scansione. La data e l'ora suggerite corrispondono a quelle correnti (in base alle informazioni di sistema). È possibile selezionare un'altra ora.
5. Per impostazione predefinita, l'attività è impostata su **Abilitato**. Rimuovere il segno di spunta per disabilitarla.
6. Fare clic su **Crea**.

Tutte le attività pianificate vengono visualizzate in un elenco nella finestra di dialogo **Editor attività**. È possibile visualizzare, modificare, eseguire ed eliminare i file delle attività dalla finestra di dialogo Editor attività. Da questa finestra è possibile attivare e disattivare o eliminare le attività. Deselezionare la casella di controllo **Attiva** per disattivare un'attività. Selezionare la casella di controllo **Elimina** e fare clic su **Elimina selezionati** per eliminare un'attività.

La posizione predefinita in cui vengono memorizzati i file delle attività è `...\Programmi\Norman\Tasks`.

Rimuovi attività

Per rimuovere un'attività, selezionare una o più entità dall'elenco delle attività e fare clic su **Elimina selezionati**.

Elenco di esclusione

I file presenti nell'elenco di esclusione non vengono sottoposti a scansione. È possibile che si scelga di non sottoporre a scansione determinati file perché generano falsi allarmi o perché la scansione richiede un tempo eccessivo. Si consiglia comunque di sottoporre regolarmente a scansione i file dell'elenco di esclusione mediante scansioni pianificate o manuali.

Copyright © 1990-2010 Norman ASA

NOTA: gli elenchi di esclusione devono essere gestiti con la massima cautela, in quanto rappresentano un potenziale rischio per la protezione. Tenere presente che l'esclusione di file o aree dalla scansione è una scelta che può pregiudicare la protezione del sistema.

Usa l'elenco di esclusione

Selezionare questa opzione per attivare l'elenco di esclusione. L'**Elenco di esclusione** consente di escludere dalla scansione i file che possono interferire con gli scanner e ridurre le prestazioni del computer.

Esclusione di file e cartelle dalla scansione

Specificare i file, le directory o le unità disco da escludere dalla scansione per la ricerca di malware. Per escludere elementi dalla scansione attenersi alla seguente procedura:

- Fare clic sul simbolo di ricerca della cartella se si desidera selezionare i file e le cartelle oppure immettere un nome file, una directory o una lettera di unità nel campo di immissione.

  I caratteri jolly (*/?) sono consentiti. Posizionare il carattere jolly all'inizio o alla fine del termine da ricercare. Non posizionare il carattere jolly al centro del termine da ricercare.

NOTA: NON utilizzare apostrofi o virgolette (' o ") per specificare gli elementi da escludere.

Esempi

C:\Dir	Esclude tutti i file nella directory e nelle sottodirectory.
*.xyz	Esclude tutti i file con estensione .xyz.
esempio.exe	Esclude il file specificato, indipendentemente dalla sua posizione.
C:\System\xyz.doc	Esclude il file specificato.

- Specificare quale scanner deve utilizzare l'elenco di esclusione.
- Fare clic su **Aggiungi a elenco** per includere la voce nell'elenco di esclusione.

NOTA: Security Suite non controlla se i file, le cartelle o le unità aggiunte all'elenco di esclusione esistono realmente. Fare attenzione a immettere nomi e percorsi corretti.

Unità di rete

È possibile escludere le unità di rete se non si desidera sottoporre a scansione le condivisioni a cui si ha accesso su computer remoti. Specificare per quale scanner applicare l'esclusione.

Elimina selezionati

Per rimuovere le voci dall'elenco, selezionare la voce e fare clic su **Elimina selezionati**. Fare clic su **Salva** per confermare le modifiche.

NOTA: si consiglia di controllare regolarmente l'elenco di esclusione.

Impostazioni

Da questa sezione è possibile configurare lo scanner automatico, lo scanner manuale e la funzione Protezione Internet. Per impostazione predefinita, sia lo scanner manuale che quello automatico utilizzano Norman Sandbox. Per ulteriori informazioni su Sandbox, fare riferimento alla sezione "Sandbox" a pagina 63. Le impostazioni dello scanner manuale sono rilevanti anche per l'opzione **Esegui scansione computer**, la scansione attivata mediante il pulsante destro del mouse, lo scanner screen saver e lo scanner da riga di comando.

Copyright © 1990-2010 Norman ASA

Scanner automatico

Lo scanner automatico lavora in background e consente di proteggere in modo automatico il sistema. È un componente di controllo dei virus fondamentale e, pertanto, deve essere sempre abilitato.

Antivirus & Antispyware > Impostazioni
Guida
Impostazioni correnti: Consigliato
Personalizza impostazioni
Scanner automatico
Scanner manuale
Protezione Internet
Abilita scanner automatico
Rimuovi automaticamente i virus rilevati
Utente locale
Per l'attività del disco nel contesto dell'utente locale.
Leggi/Esegui
Scansione alla lettura/scrittura
Servizi e utenti remoti
Per l'attività del disco in base ai servizi e agli utenti remoti.
Scrivi
Scansione alla lettura/scrittura
Usa Norman SandBox
Normale
Normale: Scansione consigliata.
Esteso: Scansione più approfondita. Non per uso regolare. Se si abilita questa funzione, si potrebbe incidere sulle prestazioni e la stabilità.
Salva

Abilita scanner automatico

Selezionando e deselezionando questa opzione si avvia e si arresta lo scanner automatico. Si consiglia di abilitare sempre lo scanner automatico.

Se lo scanner automatico viene arrestato o messo in pausa dalla barra delle applicazioni, un triangolo giallo lampeggiante appare sull'icona nella barra. Fare riferimento alla sezione "Icona della barra delle applicazioni" a pagina 13. Inoltre, Windows Security Center avvisa che “Il computer può essere a rischio”.

1. Dal menu delle impostazioni dello scanner automatico, verificare che l'opzione **Abilita scanner automatico** sia selezionata. Fare clic su **Salva** per confermare le modifiche.
   - Deselezionare la casella di controllo per disabilitare lo scanner automatico.
   - Se lo scanner automatico viene disabilitato in questo modo, Norman Security Suite non visualizza alcun avviso. Tuttavia, Security Center di Windows invia un messaggio.

NOTA: deselezionando la casella di controllo Abilita scanner automatico, lo scanner rimane disabilitato fino a quando non viene nuovamente abilitato in modo manuale.

2. Dal menu della barra delle applicazioni, fare clic su **Avvia scanner automatico**.
   - Questa opzione passa da **Avvia scanner Automatico** a **Interrompi scanner Automatico** e viceversa.
   - Lo scanner, se interrotto manualmente, viene abilitato la prossima volta che il computer viene riavviato o quando viene installato un aggiornamento di Security Suite.

Rimuovi automaticamente i virus rilevati

La funzione di scansione rileva e ripara tutti i tipi di virus. Se possibile, il file infetto viene riparato prima di essere utilizzato nell'applicazione. Se la riparazione non riesce, viene rifiutato l'accesso al file infetto. Se un file contiene esclusivamente elementi di malware verrà eliminato interamente.

Copyright © 1990-2010 Norman ASA

Modalità utente

La sezione relativa alle modalità dell'utente è suddivisa in due moduli 'Utente locale' e 'Servizi e utenti remoti'. Normalmente, per le workstation viene utilizzata la modalità **Utente locale**, mentre per il server viene utilizzata la modalità **Servizi e utenti remoti**. Le impostazioni predefinite garantiscono una protezione sufficiente per la maggior parte delle situazioni. Si consiglia di non modificarle se non si è completamente in grado di gestirne le conseguenze.

Utente locale

- **Leggi/Esegui**
  - Indica allo scanner automatico di sottoporre a scansione tutti i file prima che vengano utilizzati.
  - Esempio: se un utente fa doppio clic su un file .doc, lo scanner automatico controlla il file e l'applicazione che viene avviata (in questo caso, MS Word).
- **Scansione alla lettura/scrittura**
  - Indica allo scanner automatico di sottoporre a scansione i file aperti per la scrittura, ad esempio, quando un utente scarica un file da Internet.
  - Se è stata selezionata la scansione alla **lettura/esecuzione**, è possibile scaricare e salvare un file infetto sul disco. Tuttavia, lo scanner automatico non rileverà il virus all'apertura del file.

Servizi e utenti remoti

Questa modalità si applica a qualsiasi computer XP/Vista/Windows 7 disconnesso che può agire teoricamente come un server. In questo punto, è possibile scegliere se si desidera sottoporre a scansione i file prima che vengano utilizzati e/o quando vengono creati nuovi file oppure quando vengono modificati dei file esistenti. In altre parole, si seleziona una strategia per la scansione automatica che ha effetto quando si salvano file scaricati da Internet o da server FTP, quando un altro computer scrive i file su una condivisione di rete sul computer e così via.

- **Scrivi**
  - Indica allo scanner automatico di sottoporre a scansione i file che vengono salvati sul disco, ad esempio, quando un utente salva un file su un server. In questo caso, lo scanner automatico sul server sottoporrà a scansione il file.
- **Scansione alla lettura/scrittura**
  - Questa opzione viene utilizzata raramente. Solitamente, risulta utile se un server viene infettato, ad esempio, in seguito a un mancato aggiornamento della funzione di scansione. Esegue la scansione sia alla lettura che alla scrittura per impedire che l'infezione si diffonda ulteriormente nella rete.

Usa Sandbox

La funzionalità Sandbox consente di rilevare virus nuovi o sconosciuti. Selezionare questa opzione per attivare la ricerca di nuove varianti di virus. La funzionalità Sandbox è particolarmente attiva nella ricerca di nuovi worm e virus negli ambienti e-mail, di rete e peer to peer, ed è predisposta per la rilevazione di minacce alla sicurezza sconosciute.

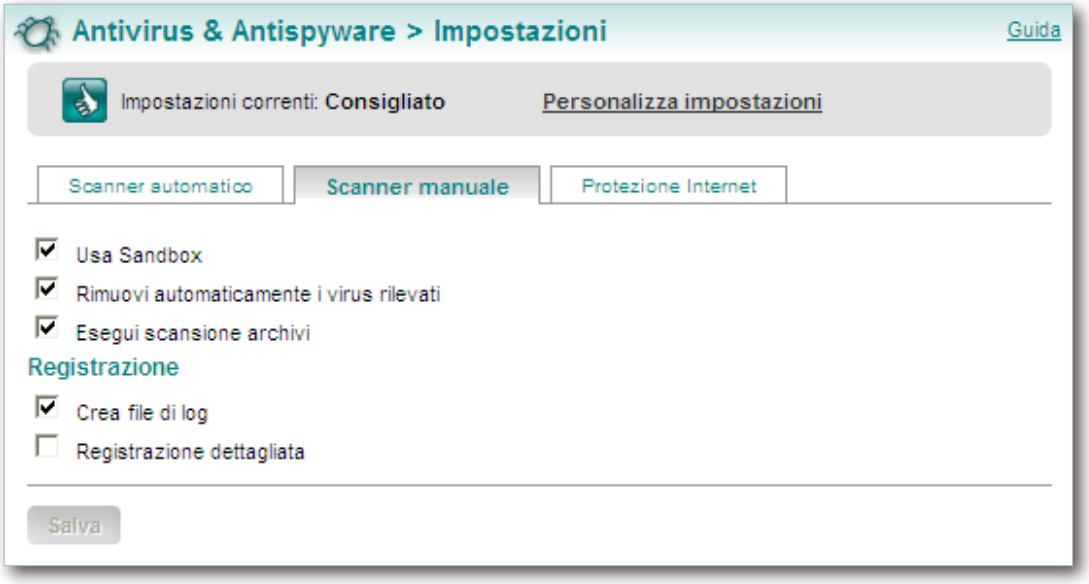
- **Disabilitato**
  - La funzione Sandbox è disattivata.
- **Normale**
  - Livello di scansione consigliato. Con questa opzione abilitata, Sandbox verifica tutte le operazioni di scrittura sia per gli utenti locali che per gli utenti remoti e i servizi.
- **Esteso**
  - In una situazione critica è possibile selezionare questa modalità se, ad esempio, si verifica un outbreak di un virus nel sistema e non è disponibile alcun rilevamento basato sulla firma per un periodo di tempo limitato. Sandbox eseguirà una verifica sia in lettura che in esecuzione. Quando l'opzione è selezionata, i tempi di scansione aumentano, tuttavia in genere le prestazioni del sistema non risultano ridotte in maniera significativa.

Fare clic su **Salva** per confermare le modifiche.

Copyright © 1990-2010 Norman ASA

Scanner manuale

Utilizzare lo scanner manuale per sottoporre a scansione determinate aree del computer. La scansione di un'intera unità disco rigido impiega diverso tempo. Per eseguire scansioni periodiche di intere unità, cartelle o file selezionati, si consiglia di impostare scansioni pianificate. Utilizzare l'Editor attività e abilitare lo scanner screen saver in modo che le scansioni vengano eseguite automaticamente durante i periodi di minore attività o di inattività. Infine, è possibile fare clic con il pulsante destro del mouse su un oggetto di file system per avviare lo scanner manuale. Tutti i metodi di scansione utilizzano le impostazioni dello scanner manuale.



Usa Sandbox

La funzionalità Sandbox consente di rilevare virus nuovi o sconosciuti. Selezionare questa opzione per attivare la ricerca di nuove varianti di virus. La funzionalità Sandbox è particolarmente attiva nella ricerca di nuovi worm e virus negli ambienti e-mail, di rete e peer to peer ed è predisposta per la rilevazione di minacce alla sicurezza sconosciute. Quando l'opzione è selezionata, i tempi di scansione aumentano, tuttavia in genere le prestazioni del sistema non risultano ridotte in maniera significativa.

Rimuovi automaticamente i virus rilevati

L'applicazione tenterà la rimozione del virus dal file infetto. Selezionare questa opzione per la riparazione automatica dei file infetti. La maggior parte dei virus può essere rimossa all'istante, salvo il caso dei virus del settore di avvio. In tal caso, verrà sempre richiesto un intervento dell'utente. Se un file contiene esclusivamente elementi di malware verrà eliminato interamente.

Esegui scansione archivi

Selezionare questa opzione per includere nella scansione i file archivio (file compressi). Attualmente sono supportati i seguenti formati: ACE, APPLE_SINGLE, ARJ, BZIP2, CAB, GZ, LZH, MAIL, RAR, RAR3, SFXZIP, TAR, ZIP e 7Z.

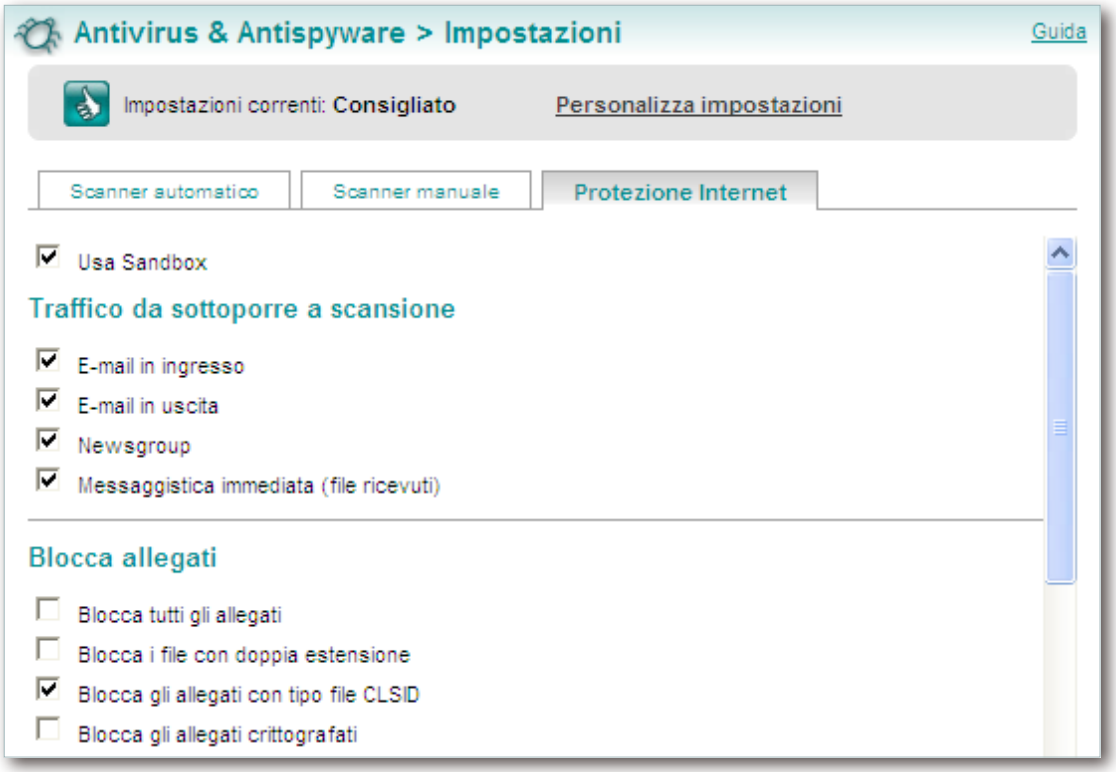
Registrazione

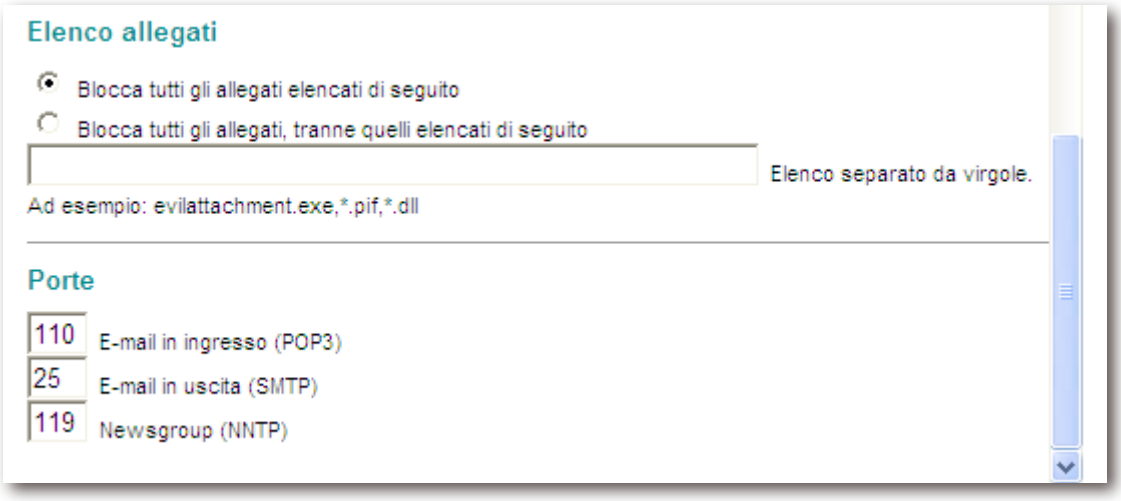
- **Crea file di log**
  Crea un file di log nella cartella C:\Programmi\Norman\Logs ogni volta che si esegue una scansione manuale. Se si deseleziona questa opzione, per le scansioni manuali non viene generato un file di log. Questa opzione è selezionata per impostazione predefinita.
- **Registrazione dettagliata**
  Genera un report dettagliato, che specifica i file sottoposti a scansione, il tempo necessario per la scansione di ciascun file, lo stato e così via.

Copyright © 1990-2010 Norman ASA

Protezione Internet

Questo filtro protegge dai virus che si diffondono attraverso la posta Internet e i lettori di news. La maggior parte dei virus segnalati attualmente utilizza meccanismi che ne consentono la diffusione attraverso l'e-mail. Questo filtro è progettato per intercettare le news e la posta in ingresso e in uscita nonché rimuovere o bloccare tutti gli allegati infetti con contenuto indesiderato. Inoltre, è in grado di sottoporre a scansione i messaggi e-mail per rilevare virus noti nonché di bloccare gli allegati in base al contenuto e alle estensioni dei file.





Usa Sandbox

La funzionalità Sandbox consente di rilevare virus nuovi o sconosciuti. Selezionare questa opzione per attivare la ricerca di nuove varianti di virus. La funzionalità Sandbox è particolarmente attiva nella ricerca di nuovi worm e virus negli ambienti e-mail, di rete e peer to peer ed è predisposta per la rilevazione di minacce alla sicurezza sconosciute. Quando l'opzione è selezionata, i tempi di scansione aumentano, tuttavia in genere le prestazioni del sistema non risultano ridotte in maniera significativa. Per ulteriori informazioni su Sandbox, fare riferimento all'Appendice A a pagina 63.

Copyright © 1990-2010 Norman ASA

Traffico da sottoporre a scansione

Selezionare gli elementi del traffico Internet da sottoporre a scansione. Per impostazione predefinita vengono sottoposti a scansione tutti gli elementi.

- **Posta in arrivo (POP3)**
  - Effettua la scansione di tutti i messaggi e-mail ricevuti da altri utenti. Anche le persone fidate o i colleghi di lavoro potrebbero non accorgersi che il loro sistema è stato attaccato da un virus.
- **Posta in uscita (SMTP)**
  - Effettua la scansione di tutti i messaggi e-mail inviati dal sistema. Se il computer è infettato da malware e non si è a conoscenza dell'infezione, si potrebbe inviare inavvertitamente messaggi e-mail infetti ad amici o colleghi.
- **Newsgroup (NNTP)**
  - Effettua la scansione del traffico generato tra il computer e gli altri partecipanti al gruppo/forum al quale si sta partecipando.
- **Messaggistica immediata (file ricevuti)**
  - Effettua la scansione dei trasferimenti di file durante le sessioni di messaggistica immediata con MSN Messenger e Windows Messenger. Quando l'opzione è selezionata, i file in ingresso vengono sottoposti a scansione per ricercare eventuali elementi di malware. Se un file è infetto un messaggio popup segnala l'infezione.
  - Vengono sottoposti a scansione solo i trasferimenti di file e, quindi, i collegamenti infetti continuano a costituire una minaccia.

Tenere presente che la scansione dei file trasferiti avviene quando tali file vengono salvati nella directory ...\File temporanei Internet**. Se viene rilevato malware, si tratta probabilmente di un file TMP messo in quarantena. Per ripristinare un file TMP in quarantena, selezionare il file desiderato, scegliere l'opzione** Salva con nome **dal menu popup visualizzato facendo clic con il pulsante destro del mouse e salvare il file con nome ed estensione originali. Vedere la sezione "Quarantena" a pagina 18.**

Blocca allegati

Questa funzionalità è particolarmente utile in presenza di worm inviati tramite e-mail identificabili in base al nome file. Il blocco degli allegati consente inoltre di rifiutare i tipi di file che non si desidera ricevere nella casella di posta. Quando un allegato viene bloccato, viene spostato nell'area di quarantena, ma non eliminato. È possibile bloccare gli allegati in base al nome o all'estensione specificandoli in modo esatto. Di seguito una breve spiegazione delle opzioni di configurazione disponibili.

- **Blocca tutti gli allegati**
  - Tutti gli allegati vengono bloccati.
- **Blocca i file con doppia estensione**
  - Molti worm e virus di posta elettronica applicano una tecnica che prevede l'aggiunta di un'estensione aggiuntiva, ad esempio **Nomefile.jpg.vbs**. La maggior parte dei client e-mail nasconde la seconda estensione, pertanto l'allegato viene visualizzato solo con l'estensione JPG. Tuttavia, questa funzione non è utilizzata solo dai virus. File provenienti da una fonte sicura con nomi quali **File.hlp.zip** ed **Elenco_attività_20.dec.doc** vengono considerati come file con estensione doppia.
- **Blocca gli allegati con tipo file CLSID**
  - Alcuni dei worm e virus inviati tramite e-mail più recenti utilizzano la tecnica CLSID per fuorviare gli scanner e-mail e il software di blocco. Utilizzano una funzionalità di Windows che consente di sostituire un'estensione .exe con un'estensione {...} e quindi evitano il blocco dei file con estensione EXE. Dal momento che per gli allegati normali questo tipo di estensione non viene utilizzato, in questi casi il file viene bloccato automaticamente.
- **Blocca gli allegati crittografati**
  - A seconda degli strumenti utilizzati, la scansione di virus nei file compressi o crittografati risulta solitamente più difficile rispetto agli allegati in formato normale. Pertanto, l'applicazione antivirus offre l'opzione di bloccare tali allegati immediatamente.

Copyright © 1990-2010 Norman ASA

Elenco allegati

Utilizzare questa funzione per selezionare gli allegati che si desidera bloccare o certificare. È possibile immettere il nome esatto di un allegato oppure utilizzare il carattere jolly (*) per bloccare estensioni specifiche. L'estensione verrà visualizzata nella casella di riepilogo, in cui sarà poi possibile modificarla o eliminarla.

Ad esempio, immettere `*.exe` per bloccare o consentire tutti gli allegati con estensione EXE. Posizionare il carattere jolly all'inizio o alla fine del termine da ricercare. Non posizionare il carattere jolly al centro del termine da ricercare.

- **Blocca tutti gli allegati elencati di seguito**
  - Tutti i nomi salvati nell'elenco mediante l'opzione **Salva** vengono **BLOCCATI**.
  - Fare clic su **Salva** per confermare.
- **Blocca tutti gli allegati tranne quelli elencati di seguito**
  - Tutti i nomi salvati nell'elenco mediante l'opzione **Salva** vengono **ACCETTATI**.
  - Fare clic su **Salva** per confermare.

NOTA: è molto importante distinguere bene queste due opzioni, perché rappresentano due estremi: BLOCCARE tutto ciò che è riportato nell'elenco o ACCETTARE tutto ciò che è riportato nell'elenco.

Fare riferimento al file della Guida in linea dell'applicazione per ulteriori informazioni su questo argomento.

Rimozione di voci

Selezionare una o più voci e fare clic su **Rimuovi selezionati**. Fare clic su **Salva** per confermare.

Porte

Tra i numerosi protocolli per comunicazione tra computer alcuni sono essenziali per l'utilizzo di Internet. Per motivi di standardizzazione, i protocolli dispongono di numeri di porta preassegnati.

Numeri di porta

Alcuni protocolli per le comunicazioni tra computer sono indispensabili per l'utilizzo di Internet. Per motivi di standardizzazione, i protocolli dispongono di numeri di porta preassegnati. Nella sezione Traffico da sottoporre a scansione, selezionare il traffico Internet di cui effettuare la scansione. La finestra identifica ad esempio i protocolli necessari per l'invio e la ricezione di e-mail e i numeri di porta corrispondenti sul computer, in base agli standard del settore.

È possibile che a uno o più protocolli supportati elencati in questa finestra di dialogo sia stato assegnato un numero di porta diverso. In tal caso, è necessario immettere il numero di porta effettivo dei protocolli interessati.

I protocolli elencati di seguito sono quelli supportati al momento. L'elenco verrà aggiornato quando necessario. I numeri di porta e le funzioni corrispondenti sono già specificati nella finestra di dialogo:

- **E-mail in ingresso (POP3)**
  (Porta 110) POP è l'abbreviazione di Post Office Protocol.
- **E-mail in uscita (SMTP)**
  (Porta 25) SMTP è l'abbreviazione di Simple Mail Transfer Protocol.
- **Newsgroup (NNTP)**
  (Porta 119) NNTP è l'abbreviazione di Network News Transfer Protocol.

Copyright © 1990-2010 Norman ASA

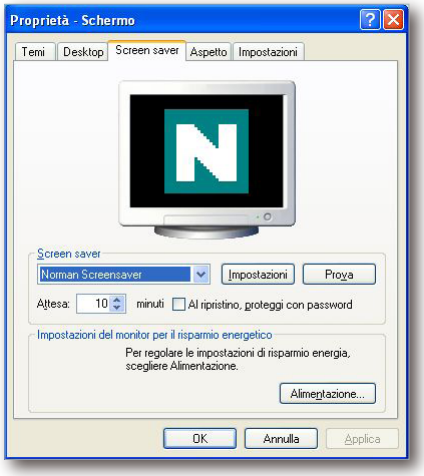
Altri metodi di scansione

Abilita scanner screen saver

Se si seleziona lo scanner screen saver, durante i periodi di inattività viene eseguita una ricerca dei virus nel sistema. Il periodo di inattività è il tempo durante il quale non viene eseguita alcuna operazione nel sistema, ad esempio non viene premuto alcun tasto o il mouse non viene spostato.

Lo scanner manuale inizierà una scansione di tutte le unità disco rigido una volta avviato lo screen saver. Non appena il computer viene attivato, ad esempio spostando il mouse o premendo un tasto, la scansione viene terminata. Se la scansione non è stata completata, alla successiva attivazione verrà ripresa dal punto in cui è stata interrotta.

1. Visualizzare la schermata **Antivirus & Antispyware** e selezionare **Abilita scanner screen saver**.
   - Viene visualizzata la finestra delle proprietà dello schermo del pannello di controllo di Windows.



2. Selezionare **Norman Screensaver** dall'elenco a discesa **Screen saver**.
   - Fare clic su **Prova** per visualizzare lo screen saver.
   - Spostando il mouse o premendo un tasto l'anteprima termina.
3. Fare clic su **OK** per confermare le modifiche.

La prossima volta che il sistema sarà inattivo e lo screen saver Norman verrà attivato, lo scanner manuale avvierà la scansione dei dischi rigidi, visualizzando continuamente lo stato di avanzamento. Spostando il mouse o premendo un tasto la scansione da screen saver viene interrotta.

NOTA: questa scansione utilizza le stesse impostazioni dello scanner manuale.

Scansione con il pulsante destro del mouse

In questo caso, lo scanner manuale avvia una scansione del file o della cartella selezionata mediante il menu popup di Windows visualizzato facendo clic con il pulsante destro del mouse.

- Fare clic con il pulsante destro del mouse su un file o una cartella.
  - Ad esempio, in Esplora Risorse o sul desktop.
- Selezionare **Scansione antivirus** dal menu popup.
- Viene visualizzata la finestra di dialogo **Scanner manuale**. È possibile utilizzare l'opzione **Sfoglia** per individuare un altro file o un'altra cartella da sottoporre a scansione e selezionare **Avvia**, **Pausa** o **Interrompi** rispettivamente per avviare, sospendere o arrestare il processo di scansione.

Scansione da riga di comando

Lo Scanner da riga di comando è un'alternativa alla scansione eseguita dall'interfaccia utente ed offre la possibilità di eseguire dei processi batch ed altre operazioni di scansione dalla riga di comando. Lo scanner da riga di comando è un'alternativa valida per utenti esperti di questo ambiente.

Copyright © 1990-2010 Norman ASA

Lo scanner da riga di comando ha la stessa funzionalità di base degli scanner attivati da menu e non dipende da altri moduli. Può anche essere eseguito da file batch.

Avvio della scansione da riga di comando

1. Avviare una sessione del prompt dei comandi.
   - Selezionare **Start** > **Esegui**.
   - Immettere CMD e fare clic su **OK** o premere **Invio**.
2. Selezionare la directory in cui risiede l'applicazione Antivirus & Antispyware.
   - La posizione predefinita è `C:\Programmi\Norman\nvc\bin\`
3. Immettere i parametri desiderati e premere Invio.
   - Per un elenco dei parametri disponibili, immettere:
     ```
     nvcc /?
     ```
   - La sintassi è:
     ```
     nvcc [unità]:[percorso] [/parametri] [Invio]
     ```
   - Ogni parametro utilizzato deve essere preceduto da uno spazio.

Copyright © 1990-2010 Norman ASA

Personal Firewall

Completare la procedura d'installazione guidata (vedere "Installazione guidata" a pagina 12). Aprire l'applicazione Security Suite e selezionare **Personal Firewall** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione e alla sezione "Personal Firewall" a pagina 6 per una descrizione dello scopo e della funzione dell'applicazione. Fare riferimento alla sezione "Installazione guidata" a pagina 12 per informazioni su come inizializzare l'applicazione Personal Firewall.

Pagina principale

NORMAN SecuritySuite
Pagina principale
Antivirus & Antispyware
Personal Firewall
Strumenti avanzati
Impostazioni
Antispam
Parental Control
Privacy Tools
Intrusion Guard
Installa e aggiorna
Centro di supporto
Personal Firewall
Guida
Impostazioni correnti: Consigliato
Personalizza impostazioni
Bloccato 0 connessioni in ingresso
Bloccato 0 connessioni in uscita
Bloccato 0 scansioni porte
Disabilita il Personal Firewall
Personal Firewall in esecuzione.
Blocca
Blocca l'accesso alla rete/Internet.
Cancella regole sessione
Elimina le regole firewall temporanee create dall'ultimo riavvio.
Cancella regole di blocco
Se una delle applicazioni non è in grado di accedere a Internet, è possibile cancellare tutte le regole di blocco. La prossima volta che si accede a Internet, verrà visualizzata una richiesta.
Strumenti avanzati
Utility di log in tempo reale e Visualizzatore porte avanzato.

In questo capitolo viene descritto come configurare l'applicazione firewall, creare regole per controllare applicazioni in entrata e in uscita, visualizzare il traffico e altro ancora. L'applicazione distingue tra utenti inesperti ed esperti. L'utente inesperto segue una procedura guidata per l'installazione, mentre l'utente esperto può eseguire una configurazione dettagliata delle impostazioni avanzate.

Personalizza impostazioni

Fare clic su questa opzione per modificare i valori predefiniti. Fare riferimento alla sezione "Impostazioni" per l'applicazione Personal Firewall a pagina 39. Per informazioni generali sulla selezione delle impostazioni consigliate o personalizzate, fare riferimento alla sezione "Impostazioni di Security Suite" a pagina 15.

Statistiche

Le statistiche visualizzano informazioni sulle connessioni in ingresso e in uscita e sulle scansioni delle porte.

- **Connessioni in ingresso bloccate**
  Un tentativo di connessione al computer è stato bloccato, probabilmente perché nel computer non è installato il software necessario. Tali connessioni sono raramente di natura dannosa. Si tratta in genere di richieste server legittime.
- **Connessioni in uscita bloccate**
  Numero di connessioni in uscita che sono state bloccate da una o più regole. Se il numero è elevato, è consigliabile verificare che le regole corrispondenti siano corrette.
- **Scansioni porte bloccate**
  Visualizza il numero di tentativi sistematici di scansione per il rilevamento di porte aperte. Talvolta i virus effettuano la scansione alla ricerca di porte aperte al fine di propagarsi. Tale operazione può tuttavia essere stata eseguita anche da software di amministrazione legittimo.

Copyright © 1990-2010 Norman ASA

Disabilitazione/abilitazione Personal Firewall

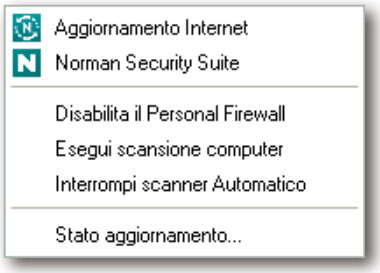
Fare clic sul collegamento per abilitare o disabilitare il Personal Firewall. È possibile abilitare o disabilitare il Personal Firewall dalla pagina principale dell'applicazione o dal menu della barra delle applicazioni.

- Visualizzare la pagina principale di Personal Firewall e selezionare **Disabilita il Personal Firewall**.

NOTA: Security Center di Windows visualizza un avviso quando il firewall viene disabilitato.

oppure

- Fare clic con il pulsante destro del mouse sull'icona della barra delle applicazioni e selezionare **Disabilita il Personal Firewall**.



NOTA: tale opzione non è disponibile in Windows Vista, dove occorre disabilitare e abilitare Personal Firewall dalla console.

Blocca

Fare clic sul collegamento per bloccare o sbloccare tutto l'accesso alla rete, incluso Internet. Questa funzione può risultare utile quando si lascia acceso il computer anche mentre non si è presenti.

Cancella regole sessione

Selezionare questa opzione per eliminare regole temporanee del firewall dall'ultimo riavvio del computer. Regole temporanee del firewall vengono create durante una sessione, ad esempio tra due riavvii del computer, quando si seleziona **si applica a questa sessione** dalla finestra popup del firewall. Questa finestra appare quando occorre decidere se consentire o rifiutare un'azione. Ad esempio, quando un programma prova a connettersi a Internet. Verrà richiesto di confermare la rimozione delle regole.

Cancella regole di blocco

Se non si riesce a connettersi a Internet o alla rete, è possibile che una regola blocchi la connessione. Fare clic su questa opzione per rimuovere tutte le regole di blocco. La volta successiva che si accede a Internet verrà visualizzata una richiesta.

Strumenti avanzati

Vedere la sezione seguente.

Copyright © 1990-2010 Norman ASA

Strumenti avanzati

Gli strumenti avanzati sono l'Editor regole, l'Utility di log in tempo reale, il Visualizzatore porte avanzato e la funzione per l'esportazione e l'importazione delle regole di Personal Firewall. Questi strumenti consentono di gestire le funzionalità avanzate dell'applicazione.

Gli strumenti avanzati sono destinati a utenti esperti. L'unica eccezione è l'Editor regole in modalità guidata, che è perfetta anche per gli utenti inesperti. È possibile passare dalla modalità guidata alla modalità avanzata nella finestra di dialogo Editor regole.

È possibile modificare o definire le regole utilizzando l'apposito Editor. Le regole del firewall sono necessarie per consentire ad applicazioni affidabili di accedere a Internet e per bloccare le connessioni non affidabili. Il firewall utilizza anche tecniche di stealthing avanzate che rendono il computer invisibile e non rilevabile da Internet. È possibile monitorare le attività del computer utilizzando l'Utility di log in tempo reale e il Visualizzatore porte avanzato.

Personal Firewall > Strumenti avanzati
Guida
Editor regole
Visualizza e modifica le regole permanenti.
Utility di log in tempo reale-
Dettagli di configurazione delle attività correlate alla rete.
Visualizzatore porte avanzato
Visualizzare lo stato delle porte e modificare le regole corrispondenti.
Esporta regole Personal Firewall
Esegue il backup delle regole e delle impostazioni del Personal Firewall.
Importa regole Personal Firewall
Ripristina un backup delle regole e delle impostazioni del Personal Firewall. Le regole esistenti vengono sovrascritte.

Editor regole

Le regole sono necessarie per consentire ad applicazioni "attendibili" l'accesso a Internet e quindi molti programmi dipendono da tali regole oggi. Il firewall ha definito alcune regole per i programmi affidabili installati sul computer al momento dell'esecuzione dell'installazione guidata. Tuttavia, è possibile che siano stati installati programmi che il firewall non ha riconosciuto o che sono stati acquistati dopo l'installazione del firewall. Quando un programma di questo tipo prova a connettersi alla rete, il Personal Firewall visualizza un messaggio popup che informa sull'azione tentata in modo che l'utente possa decidere se consentire o rifiutare tale azione.

NORMAN SecuritySuite
File HOSTS modificato
Il file HOSTS è stato appena modificato. Questo file converte un nome quale www.norman.com in un indirizzo IP e, se modificato da un programma dannoso, può essere utilizzato per indirizzare il computer a un indirizzo errato. La modifica del file è stata intenzionale?
Rifiuta
Consenti
Visualizza modifiche

Copyright © 1990-2010 Norman ASA

Personal Firewall non consente di creare regole in ingresso. Le regole in ingresso sono gestite mediante il riconoscimento della modalità server di Personal Firewall, che crea in modo dinamico e automatico regole in ingresso basate su privilegi del server. Questo è un meccanismo intelligente nel firewall che valuta i tentativi dall'esterno di accedere a un set di porte. Le richieste legittime possono accedere solo alle porte rilevanti e vengono automaticamente chiuse quando non sono più necessarie.

Al momento dell'esecuzione dell'installazione guidata di Personal Firewall, è stata scelta l'opzione per utenti esperti o inesperti. L'Editor regole differisce in base al tipo di utente selezionato.

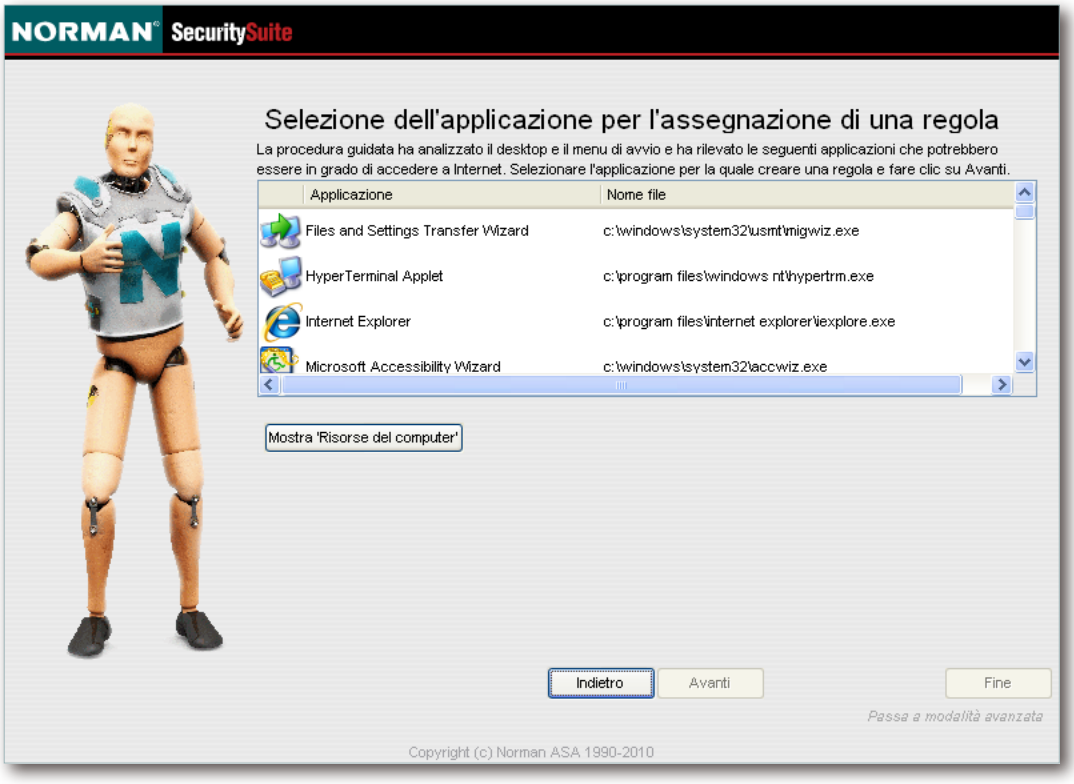
SUGGERIMENTO

PASSAGGIO TRA MODALITÀ UTENTE: nell'angolo inferiore destro della finestra di dialogo Editor regole è presente un'opzione per la selezione della modalità utente. Questa opzione può essere *Passa a modalità guidata* **e** *Passa a modalità avanzata***.**

Utente inesperto (modalità guidata)

Selezionare **Personal Firewall > Strumenti avanzati** e fare clic su **Editor regole** per aprire la finestra di dialogo Procedura guidata regola.

1. **Procedura guidata regola**
   - Selezionare **Crea una nuova regola** e fare clic su **Avanti**.


NORMAN SecuritySuite
Selezione dell'applicazione per l'assegnazione di una regola
La procedura guidata ha analizzato il desktop e il menu di avvio e ha rilevato le seguenti applicazioni che potrebbero essere in grado di accedere a Internet. Selezionare l'applicazione per la quale creare una regola e fare clic su Avanti.
Applicazione
Nome file
Files and Settings Transfer Wizard
c:\windows\system32\usmt\migwiz.exe
HyperTerminal Applet
c:\program files\windows nt\hypertrm.exe
Internet Explorer
c:\program files\internet explorer\iexplore.exe
Microsoft Accessibility Wizard
c:\windows\system32\accwiz.exe
Mostra 'Risorse del computer'
Indietro
Avanti
Fine
Passa a modalità avanzata
Copyright (c) Norman ASA 1990-2010

2. **Selezione dell'applicazione per l'assegnazione di una regola**
   - Viene visualizzato un elenco di applicazioni valide. Fare clic su un'applicazione per selezionarla. Selezionare **Mostra 'Risorse del computer'** per sfogliare il computer e identificare i programmi non presenti nell'elenco. Fare clic su **Avanti** per continuare.
3. **Qual è l'azione per l'applicazione?**
   - Selezionare **Consenti** o **Rifiuta** per consentire o meno a questa applicazione di accedere a Internet. Fare clic su **Avanti** per continuare.
4. **È un'applicazione server?**
   - Determinare se si tratta di un'applicazione server o meno. Le applicazioni server prevedono porte aperte e visibili, rendendo il computer simile a un server, e consentono, quindi, ad altri computer di connettersi. Selezionare **No** in caso di dubbio. Fare clic su **Avanti** per continuare.

SUGGERIMENTO

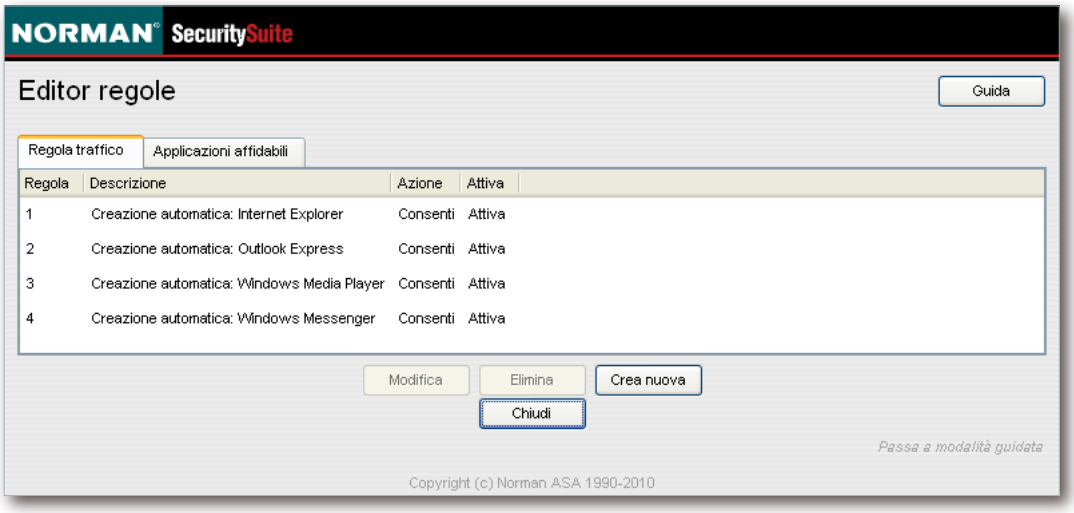
Il firewall avvisa successivamente se l'applicazione richiede privilegi server. È sempre possibile modificare una regola in un secondo momento.

Copyright © 1990-2010 Norman ASA

5. **Riepilogo**
   - Viene visualizzata una finestra di dialogo di riepilogo. Fare clic su **Fine** per generare la regola.
   - La regola ha effetto immediato una volta generata.

Utente esperto (modalità avanzata)

Selezionare **Personal Firewall > Strumenti avanzati** e fare clic su **Editor regole**. Viene visualizzata una finestra di dialogo con un elenco delle regole esistenti e del relativo stato.



1. Fare clic su **Crea nuova** e completare i campi richiesti.
2. Fare clic su **OK** per confermare.

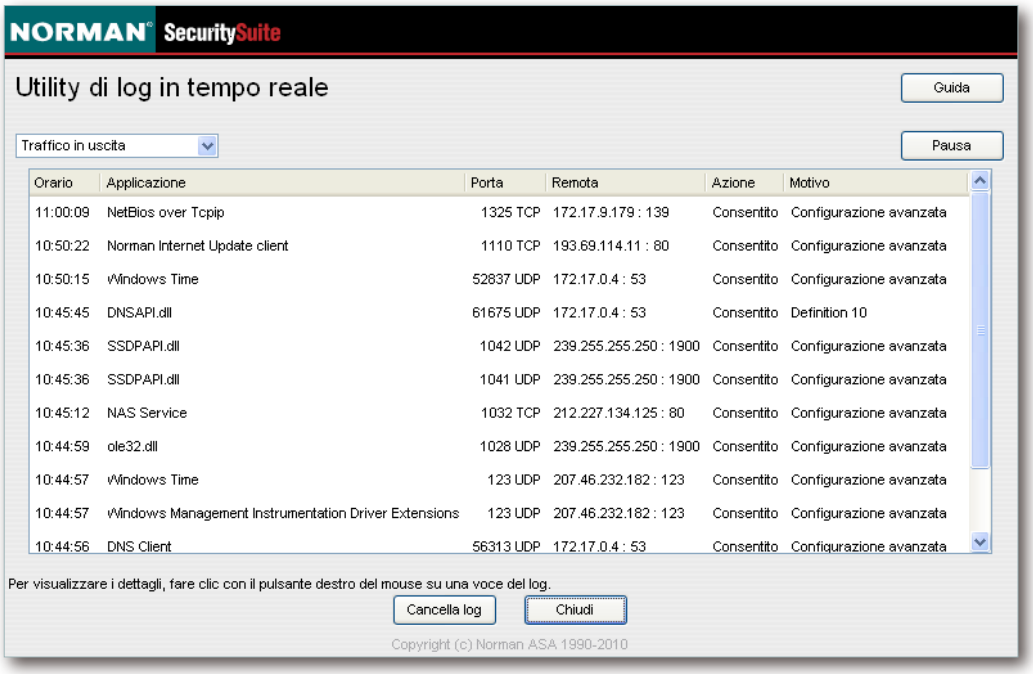
Per una descrizione dettagliata di tutti i campi, fare riferimento ai file della Guida in linea dell'applicazione.

Copyright © 1990-2010 Norman ASA

Utility di log in tempo reale

Personal Firewall utilizza tecniche di stealthing avanzate che rendono il computer invisibile e non rilevabile da Internet. È possibile tenere sotto controllo le attività sul computer utilizzando altre due funzioni: l'**Utility di log in tempo reale** e il **Visualizzatore porte avanzato**.

Selezionare **Personal Firewall > Strumenti avanzati** e fare clic su **Utility di log in tempo reale**. Fare clic con il pulsante destro del mouse per visualizzare i dettagli e possibilmente modificare la configurazione per questa applicazione.


NORMAN SecuritySuite
Utility di log in tempo reale
Guida
Traffico in uscita
Pausa
Orario Applicazione Porta Remota Azione Motivo
11:00:09 NetBios over Tcpip 1325 TCP 172.17.9.179 : 139 Consentito Configurazione avanzata
10:50:22 Norman Internet Update client 1110 TCP 193.69.114.11 : 80 Consentito Configurazione avanzata
10:50:15 Windows Time 52837 UDP 172.17.0.4 : 53 Consentito Configurazione avanzata
10:45:45 DNSAPI.dll 61675 UDP 172.17.0.4 : 53 Consentito Definition 10
10:45:36 SSDPAPI.dll 1042 UDP 239.255.255.250 : 1900 Consentito Configurazione avanzata
10:45:36 SSDPAPI.dll 1041 UDP 239.255.255.250 : 1900 Consentito Configurazione avanzata
10:45:12 NAS Service 1032 TCP 212.227.134.125 : 80 Consentito Configurazione avanzata
10:44:59 ole32.dll 1028 UDP 239.255.255.250 : 1900 Consentito Configurazione avanzata
10:44:57 Windows Time 123 UDP 207.46.232.182 : 123 Consentito Configurazione avanzata
10:44:57 Windows Management Instrumentation Driver Extensions 123 UDP 207.46.232.182 : 123 Consentito Configurazione avanzata
10:44:56 DNS Client 56313 UDP 172.17.0.4 : 53 Consentito Configurazione avanzata
Per visualizzare i dettagli, fare clic con il pulsante destro del mouse su una voce del log.
Cancella log
Chiudi
Copyright (c) Norman ASA 1990-2010

Traffico in uscita

Il log riporta l'**Ora** in cui un'**Applicazione** si è connessa a Internet, il nome del programma e la **Porta** utilizzata, indicando l'indirizzo IP **Remoto**, la porta e l'**Azione**. L'**Azione** può essere Consentito o Rifiutato. La colonna **Motivo** indica se esiste una regola permanente o di sessione per l'azione o l'applicazione, se questa impostazione è stata definita nella **Configurazione avanzata** o si basa sul timeout della richiesta utente.

Richieste privilegi di server

Il log riporta l'**Ora** in cui un'**Applicazione** ha contattato il computer da Internet, la **Porta** utilizzata, indicando l'indirizzo IP **Remoto**, la porta e l'**Azione** effettuata da Personal Firewall. L'**Azione** può essere Consentito o Rifiutato. La colonna **Motivo** indica se esiste una regola permanente o di sessione per l'azione o l'applicazione, se questa impostazione è stata definita nella **Configurazione avanzata** o se non esiste un'applicazione in ascolto. Il motivo più comune per non consentire il traffico in ingresso è il fatto che il computer non dispone del software necessario per interpretare la richiesta. In altri termini, nessuna richiesta di privilegi di server corrispondente.

Per ricevere dati da un altro computer della rete, un'applicazione apre una o più porte per l'ascolto. Tenere presente che le richieste privilegi di server non sono connessioni stabilite, bensì semplici richieste di connessione. In altri casi, tuttavia, l'applicazione apre una porta per l'ascolto al fine di ricevere una risposta da un computer al quale ha inviato dati. Il Personal Firewall autorizza automaticamente tali risposte. Un meccanismo nel Personal Firewall determina se un'applicazione ha aperto una porta deliberatamente o se ha ricevuto una richiesta indesiderata, come se si trattasse di un server. In tal caso, il Personal Firewall richiede all'utente di confermare l'assegnazione dei privilegi di server all'applicazione.

Copyright © 1990-2010 Norman ASA

Visualizzatore porte avanzato

Il Visualizzatore porte avanzato mostra una panoramica di tutta l'attività sulle porte del computer corrente. Utilizzare questa utility per controllare manualmente che nessun malware infetti il computer.

Selezionare **Personal Firewall > Strumenti avanzati > Visualizzatore porte avanzato**.

NORMAN SecuritySuite
Visualizzatore porte avanzato
Porta Stato Applicazione Scheda associata Traffico Gestito da
ingresso 1900 UDP Aperta Advanced Windows Base API (1852) 172.17.8.35 attivo Configurazione avanzata
ingresso 135 TCP Limitato a IP Generic Host Process for Win32 Services (1388) Qualsiasi attivo (0)
ingresso 123 UDP Limitato a IP Generic Host Process for Win32 Services (1512) 127.0.0.1 attivo (0)
ingresso 1028 UDP Limitato a IP Generic Host Process for Win32 Services (1512) 127.0.0.1 attivo (0)
ingresso 1041 UDP Limitato a IP Generic Host Process for Win32 Services (1512) 172.17.8.35 attivo (0)
ingresso 1042 UDP Limitato a IP Generic Host Process for Win32 Services (1512) 127.0.0.1 attivo (0)
ingresso 52837 UDP Limitato a IP Generic Host Process for Win32 Services (1512) Qualsiasi attivo (0)
Spiegazione dello stato della porta:
Chiuso Un'applicazione ha aperto questa porta ma il firewall blocca tutto il traffico verso questa porta. La porta risulta chiusa.
Protetto Sono consentite solo le risposte alle richieste in uscita; tutto l'altro traffico è bloccato. La porta è completamente bloccata.
Limitato alla LAN La porta è aperta soltanto per la rete locale (LAN). Da Internet la porta risulta completamente invisibile (stealthed).
Limitato a IP La porta è aperta soltanto a un indirizzo IP (o a un gruppo limitato di indirizzi IP). Da Internet la porta risulta completamente invisibile (stealthed).
Aperta La porta è aperta a Internet. Se una o più porte del computer sono aperte, il computer è visibile da Internet. Una porta dovrebbe essere aperta solo per software server, quali server Web e FTP. Tenere presente che, se una porta è 'aperta', il firewall non può proteggerla. Tuttavia, un'applicazione può garantirne la protezione.
Aperta (protetta) La porta è aperta in Internet ma l'applicazione ne garantisce la protezione.
Termina applicazione
Modifica regola associata
Chiudi
Copyright (c) Norman ASA 1990-2010

Le porte aperte a Internet appaiono in rosso e devono essere controllate attentamente poiché il firewall non può proteggere una porta aperta. Software server come FTP e server Web utilizzano in modo legittimo le porte aperte. Tuttavia, se un'applicazione sconosciuta è attiva su una porta aperta, è opportuno verificare.

Arresto di un'applicazione

Per arrestare un'applicazione, evidenziare la voce corrispondente e fare clic su **Termina applicazione**. L'applicazione viene terminata immediatamente anche se è possibile che venga visualizzata ancora nell'elenco per un minuto.

Accesso alla finestra per la configurazione avanzata

Evidenziare una voce e selezionare **Apri configurazione avanzata**.

NORMAN SecuritySuite
Usa Network Time Protocol e consenti il traffico sulla porta 123
OK
Annulla
Copyright (c) Norman ASA 1990-2010

NOTA: per modificare la configurazione di un'applicazione per consentire o rifiutare l'accesso, rimuovere il segno di spunta e fare clic su OK. In alternativa, selezionare la casella di controllo per consentire a un'applicazione rifiutata di accedere a Internet. Tenere presente che i pulsanti Termina applicazione e Modifica regola associata possono essere utilizzati solo per le voci 'gestite da regola'. L'opzione Apri configurazione avanzata è disponibile solo per regole gestite mediante la 'configurazione avanzata'.

Copyright © 1990-2010 Norman ASA

Esporta regole Personal Firewall

Esegue il backup delle regole di Personal Firewall. Selezionare **Esporta regole Personal Firewall** e specificare la posizione. Salvare il file su un supporto esterno per sicurezza.

Importa regole Personal Firewall

Ripristina le regole del Personal Firewall. Selezionare **Importa regole Personal Firewall** e specificare la posizione da cui ripristinare il file di backup.

Copyright © 1990-2010 Norman ASA

Impostazioni

Configura Personal Firewall

Durante l'installazione sono state create automaticamente varie regole, tra cui regole per i browser e i client e-mail più comuni, per MSN e per altri programmi che richiedono la connessione alla rete.

Selezionare **Personal Firewall > Impostazioni > Configura Personal Firewall**. Per visualizzare e/o modificare regole esistenti, fare riferimento alla sezione "Editor regole" a pagina 33.

Applicazioni in uscita

Alcune applicazioni senza regole potrebbero tentare di connettersi a Internet o alla LAN. In questa finestra di dialogo è possibile scegliere la modalità di gestione di queste applicazioni da parte di Personal Firewall. L'impostazione consigliata è **Richiedi**. Quando questa opzione è selezionata, è possibile valutare un'applicazione che, ad esempio, tenta di accedere a Internet e definire una regola. L'alternativa è **Rifiuta** e in questo caso tutti i programmi privi di una regola permanente o basata sulla sessione non possono accedere alla rete.

Privilegi di server

Alcune applicazioni senza regole potrebbero tentare di accettare connessioni da Internet. In questa finestra di dialogo è possibile scegliere la modalità di gestione di queste applicazioni da parte di Personal Firewall. L'impostazione consigliata è **Richiedi**. Quando questa opzione è selezionata, è possibile valutare se un'applicazione può accettare un invito dalla rete. L'alternativa è **Rifiuta** e in questo caso tutti i programmi privi di una regola permanente o basata sulla sessione rifiutano gli inviti dalla rete.

NOTA: nella finestra di dialogo Modifica regola è presente un'opzione che consente di concedere o rifiutare i privilegi di server per un'applicazione. Il concetto di privilegi di server è illustrato anche nell'argomento Modifica regola**.**

Impostazioni avanzate

Data la natura tecnica delle opzioni di configurazione, la modifica delle impostazioni predefinite è riservata a utenti esperti. Come regola generale, evitare di modificare le opzioni se non si conoscono lo scopo dell'opzione e i possibili effetti della modifica. Le impostazioni predefinite sono sufficienti per l'utilizzo standard del computer.

L'opzione Funzionamento del firewall viene descritta di seguito. Per una descrizione dettagliata di tutte le opzioni, fare riferimento ai file della Guida in linea dell'applicazione.

Passaggio tra modalità utente (inesperto/esperto)

Selezionare **Personal Firewall > Impostazioni > Impostazioni avanzate** e scorrere verso il basso fino alla sezione **Funzionamento del firewall.**

Questa opzione è abilitata se è stato scelto "Utente esperto" al momento dell'installazione. Se è stato scelto "Utente inesperto", viene avviata la procedura guidata per la creazione delle regole. La differenza tra i due tipi di utente è il livello di assistenza disponibile quando si creano nuove regole o si modificano le regole esistenti. Fare riferimento alla sezione "Editor regole" a pagina 33 per ulteriori informazioni su come creare le regole in due modi diversi.

Copyright © 1990-2010 Norman ASA

Antispam

Aprire l'applicazione Security Suite e selezionare **Antispam** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione e alla sezione "Antispam" a pagina 7 per una descrizione dello scopo e della funzione dell'applicazione.

Pagina principale

L'applicazione Antispam protegge da messaggi e-mail commerciali e di massa non richiesti (spam) che possono contenere minacce per il sistema. In questo capitolo viene descritto come personalizzare il filtro di spam, creare elenchi di blocco e autorizzazione, gestire messaggi e-mail filtrati, visualizzare messaggi e-mail filtrati, aggiornare intervalli e opzioni di gestione di spam.

Statistiche spam

Il grafico mostra la quantità di tentativi di spam e phishing intercettati che l'applicazione ha bloccato ogni giorno nel corso delle ultime due settimane.

Personalizza impostazioni

Fare clic su questa opzione per modificare i valori predefiniti. Fare riferimento alla sezione "Impostazioni" dell'applicazione Antispam a pagina 43. Per informazioni generali sulla selezione delle impostazioni consigliate o personalizzate, fare riferimento alla sezione "Impostazioni di Security Suite" a pagina 15.

Blocca/Consenti

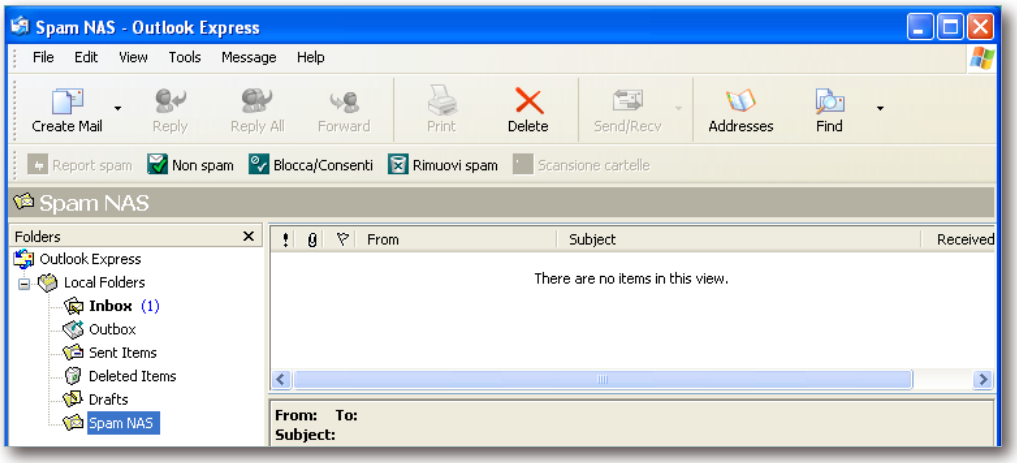
È possibile gestire singoli indirizzi e-mail utilizzando l'elenco Blocca/Consenti per indicare all'applicazione gli indirizzi che devono essere sempre consentiti o bloccati. Il metodo di filtraggio antispam non sovrascriverà mai la specifica manuale di un indirizzo (Blocca o Consenti). Fare riferimento alla sezione "Blocca/Consenti" a pagina 42.

Copyright © 1990-2010 Norman ASA

Visualizzazione di messaggi e-mail filtrati

Dall'applicazione e-mail, ad esempio Microsoft Outlook, Outlook Express o Windows Mail, è possibile visualizzare i messaggi e-mail filtrati come spam. La cartella Spam NAS viene creata quando si installa il Norman Security Suite o quando si installa uno dei client e-mail menzionati e Norman Security Suite è già installato sul computer.

Aprire il client e-mail preferito e individuare la cartella Spam NAS e il menu dell'applicazione Antispam.



- **Report spam**
  - Specifica i messaggi e-mail contrassegnati come spam. Selezionare un messaggio e-mail dalla casella della posta in arrivo e fare clic su **Report spam** dalla barra degli strumenti. Il messaggio viene spostato nella cartella **Spam NAS**.
- **Non spam**
  - Contrassegna i messaggi e-mail come non spam. Selezionare uno o più messaggi e-mail nella cartella **Spam NAS** e fare clic su **Non spam**.
- **Blocca/Consenti**
  - Blocca o consente messaggi e-mail. Selezionando questa opzione viene aperta l'applicazione Norman Antispam. Immettere uno o più indirizzi e-mail in **Blocca** o **Consenti**.
- **Rimuovi spam**
  - Cancella l'intero contenuto della cartella **Spam NAS**. Per eliminare un messaggio, fare clic con il pulsante destro del mouse e selezionare **Elimina** dal menu popup.
- **Scansione cartelle**
  - Esegue la scansione dei messaggi e-mail in entrata per rilevare eventuale spam. Selezionare una o più cartelle e fare clic su Scansione cartelle per avviare una scansione manuale. Questa opzione consente di passare tra **Scansione cartelle** e **Interrompi scansione**. Fare clic su **Interrompi scansione** per interrompere la scansione per rilevare messaggi spam.

Fare riferimento alla sezione "Gestione spam" a pagina 43 per specificare se si desidera eliminare automaticamente lo spam.

Copyright © 1990-2010 Norman ASA

Blocca/Consenti

Immettere manualmente l'indirizzo e-mail che si desidera bloccare o consentire. Specificare se l'indirizzo e-mail deve essere bloccato o consentito selezionando il pulsante di opzione rilevante accanto al campo di input.

Aggiunta/rimozione di indirizzi e-mail

Gli indirizzi e-mail vengono visualizzati in un elenco nella parte inferiore della finestra di dialogo Quando si immette un nuovo indirizzo, l'opzione **Blocca** è l'impostazione predefinita per impedire un'approvazione involontaria di un indirizzo che deve essere bloccato. In alternativa, selezionare **Consenti** per accettare il messaggio e-mail da questo mittente. È possibile modificare in qualsiasi momento i dettagli nell'elenco di indirizzi e-mail.

Aggiungi

1. Immettere un indirizzo e-mail, ad esempio, `nome1@dominio.com`
   oppure
   - Immettere diversi indirizzi e-mail separati da una virgola, ad esempio, `nome1@dominio.com, nome2@dominio.com`

   oppure
   - Immettere un intero dominio da consentire o bloccare, ad esempio, `offertefasulle.com`
   - Nota: non aggiungere il proprio dominio per evitare lo spoofing dei messaggi e-mail.
2. Selezionare **Consenti** o **Blocca** (opzione predefinita) per ogni indirizzo.
3. Fare clic su **Aggiungi** per ogni nuova voce.
4. Fare clic su **Salva** per mantenere nuovi indirizzi o domini.

Rimuovi

1. Selezionare uno o più indirizzi.
2. Fare clic su **Rimuovi selezionati**.
3. Fare clic su **Salva** per confermare le modifiche.

Modifica

1. Selezionare uno o più indirizzi.
2. Immettere le modifiche desiderate per l'indirizzo e-mail da bloccare o consentire.
3. Fare clic su **Salva** per confermare le modifiche.

Copyright © 1990-2010 Norman ASA

Impostazioni

Come le applicazioni antivirus utilizzano file di definizione dei virus per rilevare malware, le soluzioni antispam utilizzano file di definizione per filtrare messaggi e-mail non richiesti. Mentre i file di definizione dei virus contengono firme che determinano se un file è infetto o meno, le definizioni antispam utilizzano una serie di criteri per determinare la probabilità che un messaggio e-mail sia un messaggio di spam. Le definizioni di spam basano l'analisi di un messaggio e-mail sulla lingua, sulle immagini, sui colori, sui collegamenti inclusi nel messaggio nonché sull'indirizzo e-mail e IP del mittente. Non è sempre possibile concludere con assoluta certezza che un messaggio e-mail è spam.

Configura livello filtro

Se si utilizza l'indicatore e si imposta il livello del filtro su **Basso**, l'applicazione Antispam esamina i messaggi e-mail con la massima attenzione e, di conseguenza, contrassegna un numero inferiore di messaggi e-mail come spam. Allo stesso modo, se l'indicatore viene posizionato su **Alto**, un'interpretazione più ampia dei criteri di spam determina un punteggio più basso per la classificazione di messaggi e-mail come spam.

Quando si è perlopiù certi che un messaggio e-mail sia spam, ad esempio quando il mittente è incluso in una blacklist o in un database online, il messaggio viene bloccato indipendentemente dalla posizione dell'indicatore. L'impostazione predefinita **Medio** è considerata come l'impostazione più appropriata per filtrare messaggi e-mail non desiderati.

Il metodo di filtraggio antispam non sovrascriverà mai la specifica manuale di un indirizzo.

Configura controllo spam

Aggiorna definizioni spam

Selezionare la frequenza per l'aggiornamento delle definizioni di spam, ogni cinque minuti, una volta al giorno o una volta alla settimana. L'impostazione consigliata è **Ogni cinque minuti**.

Gestione spam

Questa opzione consente di scegliere se eliminare i messaggi e-mail bloccati dal filtro antispam in base alla durata o alla quantità. Le impostazioni predefinite sono **Elimina tutto lo spam dopo** [10] **giorni** ed **Elimina lo spam se il totale supera** [500] messaggi e-mail filtrati.

Fare clic su **Salva** per confermare le modifiche.

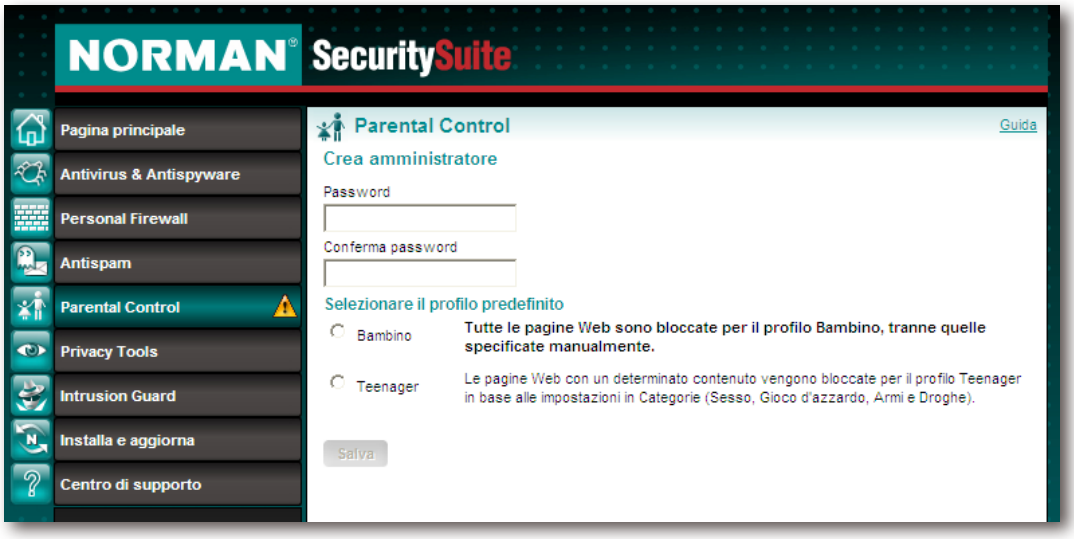
Copyright © 1990-2010 Norman ASA

Parental Control

Aprire l'applicazione Security Suite e selezionare **Parental Control** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione e alla sezione "Parental Control" a pagina 7 per una descrizione dello scopo e della funzione dell'applicazione.

Primo accesso

Al primo utilizzo di questa applicazione viene visualizzato il messaggio informativo '*Amministratore non creato!* nella pagina principale e sulla voce di menu dell'applicazione appare un triangolo di avviso giallo.



1. **Amministratore non creato**

Per accedere a Parental Control per la prima volta, occorre creare un amministratore. Immettere una password e selezionare il profilo di fallback predefinito. Fare clic su **Salva** per continuare.

Il profilo di fallback predefinito deve essere il profilo utente più basso che si desidera definire, ossia se si intende creare un profilo Bambino, anche il profilo di fallback predefinito deve essere Bambino. Solo l'amministratore può modificare gli utenti e configurare le relative impostazioni, ad esempio gli orari di accesso a Internet e gli elenchi di blocco e autorizzazioni. L'amministratore solitamente è un genitore.

Queste impostazioni possono essere modificate successivamente selezionando **Parental Control > Impostazioni.**

NOTA: la password dell'amministratore non può essere ripristinata. Accertarsi di scegliere una password facile da ricordare. La password prevede la distinzione tra maiuscole e minuscole.

2. **Connessione amministratore**

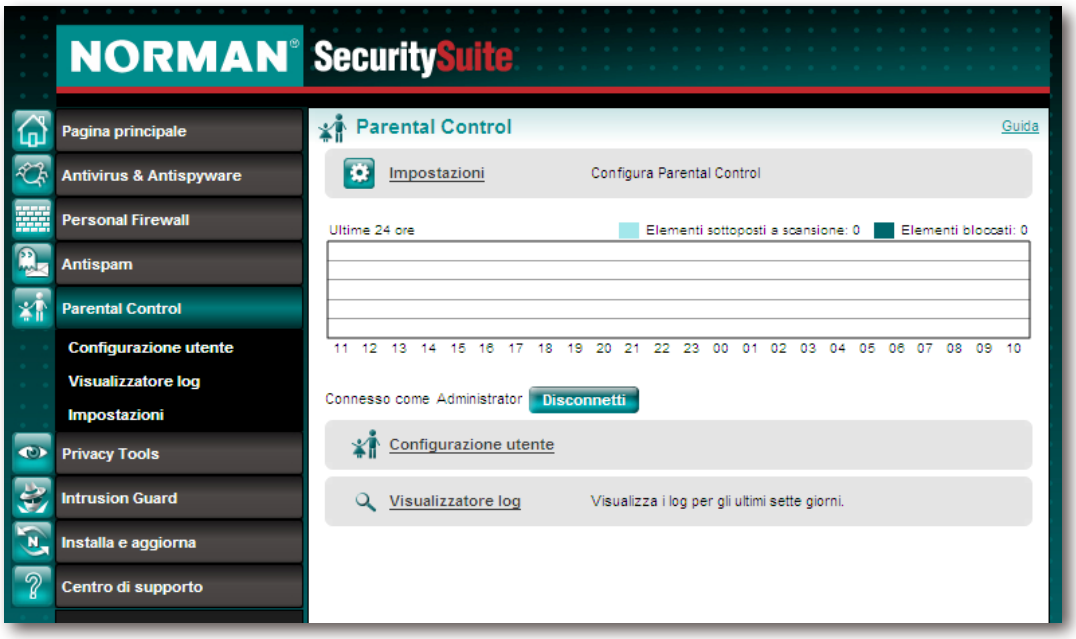
Quando viene creato un utente amministratore, viene visualizzata la pagina di connessione. Eseguire la connessione con il nome utente e la password dell'amministratore per accedere all'applicazione.

Icona della barra delle applicazioni

Un'icona sulla barra delle applicazioni indica che Parental Control è installato. Spostando il cursore del mouse sull'icona, viene indicato lo stato, ad esempio 'Parental Control: 'Amministratore' connesso'.

Copyright © 1990-2010 Norman ASA

Pagina principale



Questa applicazione blocca l'accesso a determinate categorie di siti Web e limita e pianifica l'accesso a Internet per gli utenti. In questo capitolo viene descritto come creare, configurare e gestire gli utenti nonché come visualizzare il log e pianificare l'accesso a Internet. Eseguire la connessione con il nome utente e la password dell'amministratore per accedere all'applicazione.

Impostazioni

Fare clic su questa opzione per modificare i valori predefiniti. Fare riferimento alla sezione "Impostazioni" dell'applicazione Parental Control a pagina 50.

Statistiche

Dalla pagina principale è possibile controllare le statistiche degli elementi bloccati e sottoposti a scansione.

Configurazione utente

Fare riferimento alla sezione "Configurazione utente" a pagina 46.

Visualizzatore log

Fare riferimento alla sezione "Visualizzatore log" a pagina 50.

Copyright © 1990-2010 Norman ASA

Configurazione utente

In questa finestra è possibile creare gli utenti e assegnare i profili. Per gli utenti esistenti viene elencato nome utente e profilo assegnato.

Esistono tre profili utente: **Adulto**, **Teenager** e **Bambino**. L'ultimo profilo è completamente restrittivo e consente l'accesso solo a siti Web immessi manualmente dall'amministratore nell'elenco autorizzazioni.

Adulto	Nessuna limitazione.
Teenager	Filtro basato su categorie.
Bambino	Completamente limitato.

Categorie

Le categorie si basano su un vasto repertorio di termini ed espressioni che attivano l'applicazione per l'identificazione, ad esempio, di pagine Web a contenuto erotico. I termini non sono accessibili per la visualizzazione o la modifica. Esistono quattro categorie per il profilo Teenager che bloccano l'accesso a pagine Web con contenuti di tipo **Sesso**, **Gioco d'azzardo**, **Armi** e **Droghe**. Per impostazione predefinita sono attivate tutte le categorie, tuttavia l'amministratore può deselezionare quelle che desidera consentire.

Elenco Blocca/Consenti

Per gli utenti del profilo Bambino deve esistere un elenco che contiene gli indirizzi Web dei siti a cui è possibile accedere. Per gli utenti del profilo Teenager è opzionale creare un elenco di siti bloccati e un elenco di siti autorizzati. Vedere le sezioni "Profilo Bambino predefinito" a pagina 47 e "Profilo Teenager predefinito" a pagina 47.

Formato dell'indirizzo Web

URL (Uniform Resource Locator) è il termine tecnico per un indirizzo Web. I caratteri jolly (*/?) non sono supportati negli indirizzi Web. I formati validi sono:

- http://www.newspaper.com
- www.newspaper.com
- newspaper.com

Un determinato indirizzo Web consente di visitare i livelli dei sottodomini, ma non consente mai di visitare il livello principale. Ad esempio, concedendo l'accesso a www.newspaper.com/kidsstuff non si consente di accedere al livello principale www.newspaper.com. Tuttavia, se si aggiunge l'indirizzo principale newspaper.com, saranno accessibili tutti i livelli dei sottodomini di questo indirizzo Web, ad esempio news.newspaper.com, cartoon.newspaper.com e così via.

NOTA: se l'utente segue un collegamento da una pagina consentita, tale collegamento sarà comunque accessibile. Tuttavia, non sarà possibile aprire un'altra pagina a meno che la pagina di riferimento non sia espressamente consentita.

Copyright © 1990-2010 Norman ASA

Impostazioni predefinite del profilo

Il profilo **Adulto** non prevede alcuna limitazione. I profili **Bambino** e **Teenager** sono soggetti a limitazioni e possono, quindi, essere configurati. Se un utente assegnato al profilo **Bambino** deve accedere a Internet, occorre specificare una pagina Web. Le impostazioni del profilo si applicano a tutti i membri del profilo utente. Per configurare un utente separato, fare riferimento alla sezione "Crea utente" a pagina 48.

Profilo Bambino predefinito

È necessario tenere presente che le modifiche apportate all'elenco autorizzazioni verranno applicate all'intero profilo, non solo al singolo utente. Per il profilo Bambino tutte le pagine Web sono bloccate, ad eccezione di quelle espressamente consentite; pertanto, per questo profilo le opzioni Elenco di blocco o Categoria non sono disponibili.

Aggiungi

1. Immettere un indirizzo Web autorizzato nel campo **Aggiungi indirizzo a elenco**.
   - Immettere più indirizzi separati da una virgola.
2. Fare clic su **Aggiungi** per ogni nuova voce.

Rimuovi

1. Selezionare uno o più indirizzi.
2. Fare clic su **Rimuovi selezionati**.

Profilo Teenager predefinito

È necessario tenere presente che le modifiche apportate all'elenco autorizzazioni verranno applicate all'intero profilo, non solo al singolo utente. Per questo profilo le pagine Web sono limitate in base alle Categorie e all'elenco di blocco o autorizzazioni.

Parental Control > Configurazione utente
Guida
Profilo Teenager predefinito
Nota: queste impostazioni di profilo si applicano a tutti i membri del profilo utente.
Categorie
Elenco Blocca/Consenti
Le pagine Web per il profilo Teenager vengono bloccate in base alle impostazioni in Categorie. È possibile aggiungere una o più pagine Web per fornire l'accesso alle pagine bloccate.
Aggiungi indirizzo a elenco
Consenti
Blocca
Aggiungi
Esempio: http://www.newspaper.com;www.fun.com;www.totlers.com
Indirizzi
Consenti
Blocca
Nessun elemento da visualizzare.
Rimuovi selezionati
Salva

Categorie

Tutte le categorie sono selezionate per impostazione predefinita, ossia le pagine Web con un determinato contenuto vengono bloccate per il profilo Teenager in base a queste impostazioni. Le categorie sono Sesso, Gioco d'azzardo, Armi e Droghe. L'amministratore può rimuovere il segno di spunta per consentire l'accesso a pagine Web di tale categoria. In alternativa, aggiungere una o più pagine Web all'elenco Consenti. Fare clic su **Salva** per confermare le modifiche.

Copyright © 1990-2010 Norman ASA

Elenco Blocca/Consenti

Le pagine Web per il profilo Teenager vengono bloccate in base alle impostazioni delle Categorie. È possibile aggiungere una o più pagine Web per concedere l'accesso a pagine bloccate.

Aggiungi

1. Immettere un indirizzo Web autorizzato nel campo **Aggiungi indirizzo a elenco**.
   - Immettere più indirizzi separati da una virgola.
2. Fare clic su **Aggiungi** per ogni nuova voce.
3. Selezionare il pulsante di opzione **Blocca** o **Consenti**.
4. Fare clic su **Aggiungi** per ogni nuova voce.

Crea utente

Selezionare **Crea utente** da **Parental Control > Configurazione utente**.

1. Immettere un nome per il nuovo utente e una password con relativa conferma.
2. **Selezionare il profilo predefinito** su cui basare il nuovo utente.
   - Quando si assegna un profilo a un utente, si decide quale tipo di pagine Web potrà visualizzare l'utente.
     - Adulto
       Nessuna limitazione. L'utente può accedere a qualsiasi sito Web.
     - Teenager
       Inizialmente, nessuna limitazione. Tuttavia, le impostazioni delle Categorie predefinite bloccheranno le pagine Web con argomenti o contenuti indesiderati.
     - Bambino
       È possibile visualizzare solo le pagine Web che l'amministratore ha inserito nell'elenco autorizzazioni.
3. Fare clic su **Salva** per confermare.
   - Prima di fare clic su **Salva** per creare il nuovo utente, occorre verificare che il profilo selezionato sia corretto.

Il nuovo utente viene aggiunto all'apposito elenco. Fare clic sul nome utente per configurare l'utente.

Cambia password

Modificare il nome e la password per l'utente selezionato.

Categorie

Questa selezione si applica solo a utenti con profilo Teenager. Per consentire una o più categorie per un utente con profilo Teenager, eliminare il segno di spunta dalle caselle delle categorie rilevanti. Per ulteriori informazioni, fare riferimento alla sezione "Categorie" a pagina 46 e "Profilo Teenager predefinito" a pagina 47.

Elenco Blocca/Consenti

Questa selezione si applica solo a utenti con profilo Teenager. Da qui è possibile autorizzare o bloccare indirizzi Web per l'utente. Per ulteriori informazioni, fare riferimento alla sezione "Elenco Blocca/Consenti" a pagina 46 e "Profilo Teenager predefinito" a pagina 47.

Elenco autorizzazioni

Questa selezione si applica solo a utenti con profilo Bambino. Da qui è possibile autorizzare indirizzi Web per l'utente. Fare riferimento alla sezione "Profilo Bambino predefinito" a pagina 47.

Utility di pianificazione

L'amministratore può definire in quali orari e in quali giorni della settimana un utente può utilizzare Internet. L'impostazione predefinita prevede che tutti i periodi siano consentiti (verde).

Copyright © 1990-2010 Norman ASA

1. Per bloccare l'accesso a Internet per un periodo di tempo specifico, fare clic sul periodo desiderato.
2. Fare clic e trascinare il cursore in alto, in basso, a destra o a sinistra in un movimento unico per estendere il periodo in cui si desidera rifiutare i tentativi. Allo stesso modo, trascinare la selezione per passare da **Rifiuta** (grigio) a **Consenti** (verde).
3. Fare clic su **Salva** per confermare le modifiche.

Copyright © 1990-2010 Norman ASA

Visualizzatore log

L'applicazione registra automaticamente pagine Web bloccate per utenti con profilo Teenager e Bambino. Nei log non sono visualizzate le pagine visitate dall'utente.

Il log può indicare le pagine bloccate risalenti fino a una settimana prima. Viene creato un log al giorno durante la settimana ed è possibile selezionare unicamente un giorno della settimana e non una data. L'applicazione consiglia come predefinito il giorno della settimana corrente.

Le colonne nei log indicano la data, l'ora, l'utente, il motivo del blocco e l'indirizzo URL bloccato.

Se la colonna Utente viene lasciata vuota, viene attivata la modalità fallback con nessun utente connesso.

Impostazioni

È possibile evitare che un bambino utilizzi un computer il cui accesso è stato eseguito da un adulto (se si dimentica di disconnettersi oppure è necessario allontanarsi improvvisamente dal computer). Il profilo di fallback predefinito verrà attivato dopo un periodo di inattività specificato.

Tempo di inattività prima di passare al profilo predefinito

Il periodo di inattività è il tempo durante il quale non viene eseguita alcuna operazione nel sistema, ad esempio non viene premuto alcun tasto o il mouse non viene spostato.

- Nel menu a discesa è possibile specificare quando riattivare il profilo di fallback predefinito durante il periodo di inattività del computer.
- Fare clic su **Salva** per confermare.

Imposta il profilo di fallback predefinito

È possibile selezionare Teenager o Bambino come profilo che l'applicazione deve utilizzare dopo il periodo di inattività specificato.

- **Bambino**
  Tutte le pagine Web vengono bloccate per il profilo Bambino, eccetto le pagine a cui si accede manualmente. Ciò significa che una pagina Web aggiunta per l'utente Bambino non è disponibile per l'accesso Internet.
- **Teenager**
  Le pagine Web con determinati contenuti vengono bloccate per il profilo Teenager in base alle impostazioni delle Categorie (ossia, Sesso, Gioco d'azzardo, Armi e Droghe).
- Fare clic su **Salva** per confermare.

Modifica password amministratore

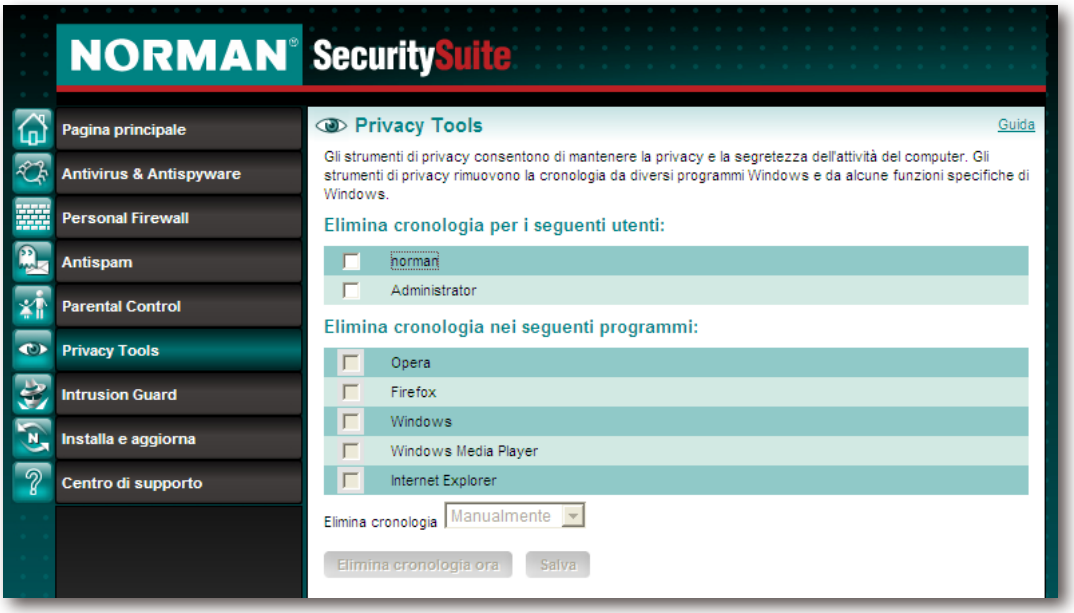
La password dell'amministratore non può essere ripristinata, ma è possibile modificarla se si conosce la precedente. Se si modifica la password amministratore, sarà necessario annotarla e conservarla in un luogo sicuro.

NOTA: tenere presente che la password prevede la distinzione tra maiuscole e minuscole.

Copyright © 1990-2010 Norman ASA

Privacy Tools

Aprire l'applicazione Security Suite e selezionare **Privacy Tools** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione e alla sezione "Privacy Tools" a pagina 7 per una descrizione dello scopo e della funzione dell'applicazione.



Questa applicazione consente di eseguire l'eliminazione sicura di file specifici. Il contenuto dei file viene cancellato in modo permanente e non può essere recuperato. È anche possibile configurare l'applicazione in modo che elimini automaticamente diversi file di log contenenti i dati personali, i cookie e la cronologia del browser. L'eliminazione di log della cronologia non ha effetti sulle impostazioni e sui segnalibri dell'applicazione.

Eliminazione della cronologia dei programmi di un utente

L'elenco di nomi utente visualizza tutti gli utenti registrati di questo computer e l'elenco dei programmi visualizza le applicazioni per le quali è possibile eliminare la cronologia.

- Selezionare uno o più nomi utente e programmi per i quali eliminare la cronologia.
- Fare clic su **Elimina cronologia ora** per confermare.

Eliminazione manuale o automatica della cronologia

È possibile eliminare la cronologia manualmente o configurare l'applicazione in modo che la cronologia venga eliminata automaticamente a intervalli regolari.

- **Manualmente**
  I log della cronologia verranno eliminati solo quando si seleziona **Elimina cronologia ora**.
- **Ogni 10 minuti** oppure **Ogni ora**.
  I log della cronologia verranno eliminati automaticamente in base alla frequenza selezionata.
- Fare clic su **Salva** per confermare.

NOTA: se si sceglie di eliminare la cronologia Manualmente**, i log verranno eliminati solo se si seleziona** Elimina cronologia ora**. I log NON verranno eliminati automaticamente.**

Copyright © 1990-2010 Norman ASA

Eliminazione sicura

Questa applicazione consente di eseguire l'eliminazione sicura di file specifici. Il contenuto dei file viene cancellato in modo permanente e non può essere recuperato.

È possibile avviare un processo di eliminazione sicura dei file semplicemente facendo clic con il pulsante destro del mouse. Verrà richiesto di confermare l'eliminazione. Viene visualizzato lo stato del processo di eliminazione e, al termine, appare un riepilogo. Per eseguire l'eliminazione sicura dei file, effettuare le seguenti operazioni:

- Selezionare uno o più file da eliminare.
- Fare clic con il pulsante destro del mouse su uno o più file.
- Selezionare **Norman Secure Delete** dal menu popup.
- Fare clic su **OK** per confermare.
- Fare clic su **OK** per chiudere la finestra del riepilogo.

Il contenuto dei file viene cancellato in modo permanente dal computer.

NOTA: l'uso del metodo di eliminazione sicura dei file richiede molto più tempo rispetto alla semplice eliminazione dei file. Ciò avviene perché ogni parte del file viene sovrascritta diverse volte per impedire il recupero di qualsiasi traccia del contenuto originale.

Se si interrompe il processo di eliminazione una volta avviato, il file verrà comunque rimosso ma non in modo permanente.

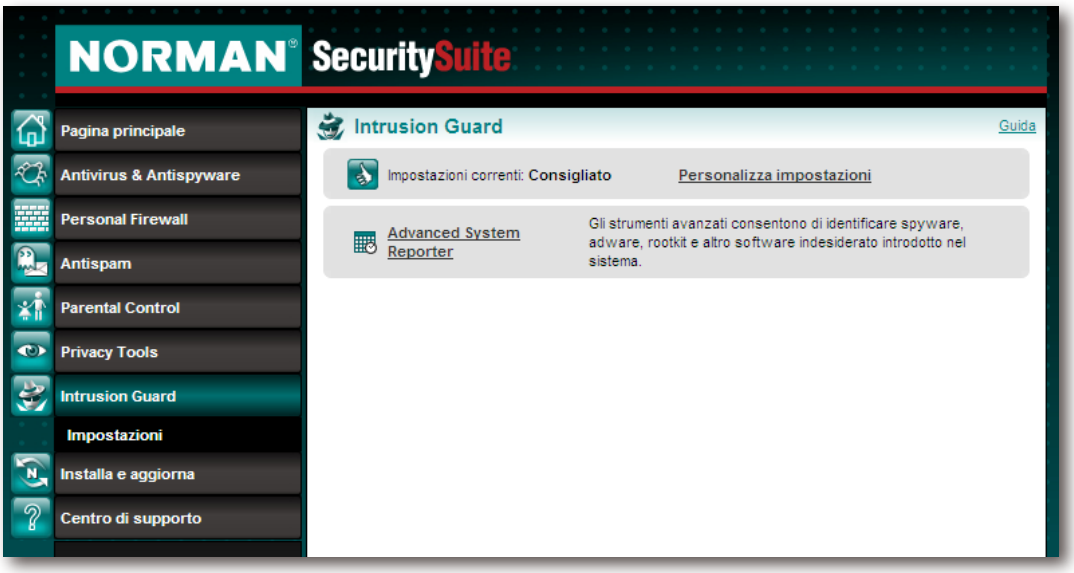
Alcuni file non possono essere eliminati. Ciò perché l'utente non dispone dell'autorizzazione in scrittura per i file o perché il file è protetto dal sistema operativo e non può essere eliminato.

Copyright © 1990-2010 Norman ASA

Intrusion Guard

Aprire l'applicazione Security Suite e selezionare **Intrusion Guard** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione e alla sezione "Intrusion Guard" a pagina 8 per una descrizione dello scopo e della funzione dell'applicazione.

Pagina principale



Questa applicazione è un sistema di prevenzione intrusioni (HIPS) basato su host destinato a utenti esperti. Gli utenti inesperti devono mantenere il prodotto configurato in base alle impostazioni consigliate che permettono l'esecuzione e la registrazione degli eventi. Solo gli eventi ad alto rischio e che sono utilizzati raramente da applicazioni legittime vengono bloccati per impostazione predefinita.

Personalizza impostazioni

Fare clic su questa opzione per modificare i valori predefiniti. Fare riferimento alla sezione "Impostazioni" a pagina 53. Per informazioni generali sulla selezione delle impostazioni consigliate o personalizzate, fare riferimento alla sezione "Impostazioni di Security Suite" a pagina 15. È consigliabile che solo utenti esperti personalizzino queste impostazioni (ossia, le impostazioni predefinite).

Advanced System Reporter

Questo strumento è destinato agli utenti esperti. La sua funzionalità consente di rilevare spyware e rootkit sconosciuti ricercando eventuali anormalità nel computer. Fare riferimento all'Appendice B a pagina 64.

Impostazioni

In questa finestra di dialogo è possibile visualizzare e modificare la configurazione dell'applicazione. Selezionare **Personalizza impostazioni** nella parte superiore della finestra di dialogo per modificare le impostazioni predefinite oppure selezionare **Impostazioni consigliate** per tornare alla configurazione predefinita.

NOTA: è consigliabile che solo gli utenti esperti modifichino le impostazioni predefinite.

Copyright © 1990-2010 Norman ASA

Driver e memoria

Intrusion Guard > Impostazioni
Guida
Impostazioni correnti: Consigliato
Personalizza impostazioni
Driver e memoria
Processi
Rete
Installazione del driver
Un driver di sistema può accedere e controllare le periferiche hardware; a tale scopo, è necessario che disponga dell'accesso completo al sistema con un livello superiore anche alle applicazioni eseguite con privilegi di amministratore. Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di installare driver sul sistema?
Richiedi
Consenti
Rifiuta
Accesso alla memoria fisica (solo 32-bit)
Mediante la gestione diretta della memoria fisica, un'applicazione può eseguire attività normalmente protette dal sistema operativo. Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di accedere alla memoria fisica?
Richiedi
Consenti
Rifiuta
Caricamento ed esecuzione di driver (solo 32-bit)
Un'applicazione dannosa può tentare di caricare un driver di sistema senza prima installarlo. Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di caricare ed eseguire driver direttamente?
Salva

I driver sono programmi del computer che operano a basso livello; questo livello è spesso denominato 'livello kernel'. I driver sono solitamente scritti per accedere e controllare l'hardware, come il monitor, la tastiera, la stampante e la scheda di rete. Per accedere all'hardware collegato al computer, i driver devono avere accesso completo al sistema. Le stesse tecniche vengono utilizzate nella scrittura di applicazioni dannose. È possibile modificare la configurazione di installazione dei driver per controllare le applicazioni a cui è consentito installare i driver sul computer.

Esistono due tecniche malware per ottenere gli stessi privilegi dei driver. Entrambe queste tecniche aggirano i meccanismi di sicurezza del sistema operativo. È altamente consigliato mantenere le impostazioni per entrambi su **Rifiuta**.

- **Richiedi**
  Verrà richiesta una conferma ogni volta che si verifica un tentativo.
- **Consenti**
  I tentativi verranno solo registrati.
- **Rifiuta**
  Nessuna applicazione, legittima o dannosa, potrà installare i driver a livello di kernel.

Copyright © 1990-2010 Norman ASA

Processi

Intrusion Guard > Impostazioni
Guida
Impostazioni correnti: Consigliato
Personalizza impostazioni
Driver e memoria
Processi
Rete
Protezione da auto-avvio
Un'applicazione può indicare al sistema operativo di avviarsi automaticamente ogni volta che il computer viene avviato o che un utente esegue l'accesso. Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di eseguire questa attività? Tenere presente che questa funzione non incide sull'esecuzione automatica di CD o penne USB.
Richiedi
Consenti
Rifiuta
Installazione del servizio
Un'applicazione può installarsi come servizio di background che fa in modo che venga eseguita ogni volta che il computer viene avviato e che l'esecuzione venga effettuata con privilegi di sistema. Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di installare un servizio?
Richiedi
Consenti
Rifiuta
Protezione processi (solo 32-bit)
Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di assumere il controllo di un altro processo mediante l'inserimento dei thread o di altro codice in tale processo?
Salva

Se un'applicazione, legittima o dannosa, viene installata sul computer, molto probabilmente verrà avviata automaticamente a ogni avvio del computer. Un programma che prevede l'avvio automatico può indicare al sistema operativo di auto-avviarsi con gli stessi privilegi dell'utente corrente oppure installare un servizio di background che viene eseguito con privilegi superiori. Questa applicazione è in grado di bloccare tali tentativi.

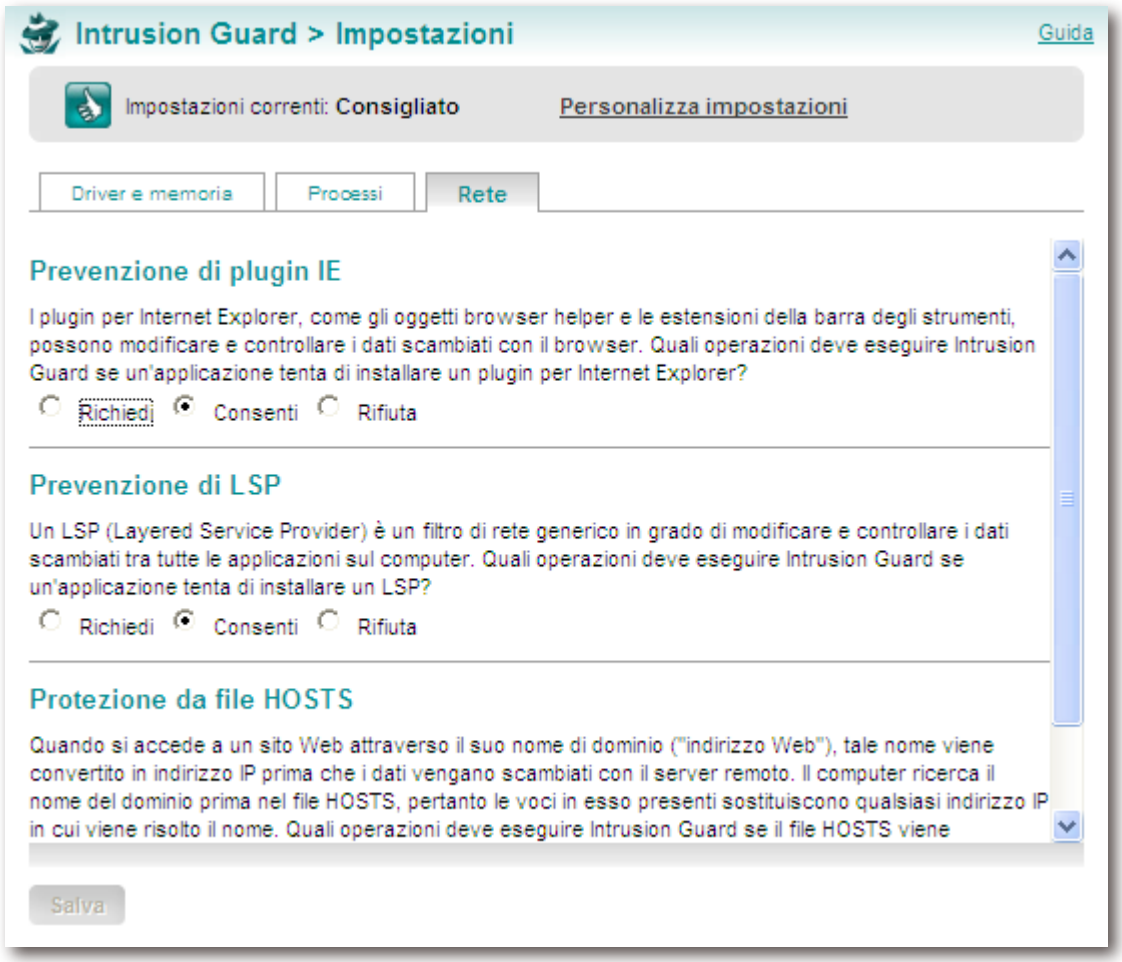
- **Richiedi**
  Verrà richiesta una conferma ogni volta che si verifica un tentativo.
- **Rifiuta**
  Nessuna applicazione, legittima o dannosa, potrà installarsi per avviarsi automaticamente all'avvio del computer.

Un programma può anche inserire codice in altri processi in esecuzione sul proprio computer oppure assumere il controllo dei processi in altro modo. Questo comportamento è tipico delle applicazioni dannose, tuttavia anche alcuni programmi legittimi utilizzano tali tecniche, ad esempio, per estendere il desktop dell'utente o per offrire altre funzioni avanzate al sistema operativo o ad applicazioni di terze parti. È possibile configurare l'applicazione in modo che rifiuti ogni tentativo o chieda conferma.

È possibile creare un elenco di applicazioni affidabili in modo da includere le applicazioni legittime che spesso funzionano in questo modo.

Copyright © 1990-2010 Norman ASA

Rete


Intrusion Guard > Impostazioni
Guida
Impostazioni correnti: Consigliato
Personalizza impostazioni
Driver e memoria
Processi
Rete
Prevenzione di plugin IE
I plugin per Internet Explorer, come gli oggetti browser helper e le estensioni della barra degli strumenti, possono modificare e controllare i dati scambiati con il browser. Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di installare un plugin per Internet Explorer?
Richiedi
Consenti
Rifiuta
Prevenzione di LSP
Un LSP (Layered Service Provider) è un filtro di rete generico in grado di modificare e controllare i dati scambiati tra tutte le applicazioni sul computer. Quali operazioni deve eseguire Intrusion Guard se un'applicazione tenta di installare un LSP?
Richiedi
Consenti
Rifiuta
Protezione da file HOSTS
Quando si accede a un sito Web attraverso il suo nome di dominio ("indirizzo Web"), tale nome viene convertito in indirizzo IP prima che i dati vengano scambiati con il server remoto. Il computer ricerca il nome del dominio prima nel file HOSTS, pertanto le voci in esso presenti sostituiscono qualsiasi indirizzo IP in cui viene risolto il nome. Quali operazioni deve eseguire Intrusion Guard se il file HOSTS viene
Salva

Mediante l'aggiunta di filtri ai moduli di rete nel sistema operativo, applicazioni dannose possono sottrarre i dati personali (ad esempio, i numeri di previdenza sociale, i dettagli della carta di credito e le password). L'adware può modificare i dati di rete inviati attraverso tali filtri, può modificare i risultati dei motori di ricerca e visualizzare pubblicità indesiderate sul desktop e incorporate nelle pagine Web visitate.

Un oggetto browser helper (BHO, Browser Helper Object) è un'estensione di Internet Explorer di Microsoft. Questo e altri plugin di Internet Explorer, come le barre degli strumenti, hanno il controllo completo sul traffico di rete con Internet Explorer e possono interagire con l'interfaccia utente.

Un LSP (Layered Service Provider) è un filtro generico nello stack di rete di Windows ed ha il controllo completo su tutto il traffico di rete del computer.

Quando si accede a un sito Web attraverso il relativo nome di dominio (indirizzo Web), tale nome viene tradotto in indirizzo IP. I dati vengono quindi inviati tra il computer e il server remoto. Il computer prima ricerca il nome del dominio nel file HOSTS. Ciò significa che le voci in tale file sovrascrivono qualsiasi indirizzo IP in cui viene risolto il nome. Applicazioni dannose possono modificare il file HOSTS e reindirizzare il traffico di rete a un sito Web dannoso (processo noto come 'pharming').

- **Richiedi**
  Viene richiesta conferma ogni volta che si verifica un evento.
- **Rifiuta**
  Tutti i tentativi di modificare il sistema e il file HOSTS e di installare un BHO o un LSP verranno interrotti.

Copyright © 1990-2010 Norman ASA

Installa e aggiorna

Aprire l'applicazione Security Suite e selezionare **Installa e aggiorna** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione.

Pagina principale

Il menu **Installa e aggiorna** visualizza, oltre ad altre opzioni, un elenco di tutti i prodotti disponibili in Security Suite. Da questo menu è possibile aggiungere o rimuovere prodotti, avviare aggiornamenti, attivare la Gestione licenza guidata e modificare la lingua dell'installazione di Norman Security Suite.

NOTA: per applicare le modifiche apportate a questa pagina è possibile che sia necessario riavviare il sistema.

Personalizza impostazioni

Fare clic su questa opzione per modificare i valori predefiniti. Fare riferimento alla sezione "Impostazioni" a pagina 58. Per informazioni generali sulla selezione delle impostazioni consigliate o personalizzate, fare riferimento alla sezione "Impostazioni di Security Suite" a pagina 15.

Prodotti con licenza

L'elenco dei prodotti con licenza visualizza i prodotti installati, il relativo stato e la data di scadenza della licenza. Da questa pagina è possibile aggiungere o rimuovere prodotti o componenti nell'elenco. Se si deseleziona una casella di controllo, il prodotto corrispondente verrà disinstallato. Nuovi prodotti o componenti eventualmente aggiunti a Norman Security Suite vengono scaricati automaticamente. Tutti i prodotti selezionati vengono automaticamente aggiornati tramite l'Aggiornamento Internet di Norman Security Suite.

NOTA: se si deseleziona la casella di controllo di un prodotto, il prodotto deselezionato verrà disinstallato e quindi non verrà mai aggiornato.

Copyright © 1990-2010 Norman ASA

Aggiornamento di tutti i prodotti

Sono disponibili aggiornamenti frequenti per definizioni di virus e file di programma. L'aggiornamento viene eseguito tramite Internet o la rete interna. Una volta scaricato il pacchetto mediante l'aggiornamento Internet, l'aggiornamento verrà installato automaticamente. Al termine dell'installazione, verrà richiesto di riavviare il computer.

- Fare clic su **Aggiorna tutti i prodotti** una volta aggiornato interamente Security Suite.

Abilitazione/disabilitazione degli aggiornamenti automatici

Gli aggiornamenti automatici sono attivati per impostazione predefinita. Questo significa che le installazioni dei prodotti vengono aggiornate ogni volta che occorre aggiornare relativi componenti o file di definizione. Per modificare le impostazioni dell'aggiornamento automatico, fare riferimento alla sezione **Impostazioni > Seleziona metodo di aggiornamento**.

NOTA: il software antivirus deve essere aggiornato frequentemente per essere certi che eventuale malware venga rilevato ed eliminato in modo efficiente.

Selezione della lingua del prodotto

È possibile modificare la lingua selezionata durante l'installazione. Selezionare la lingua preferita dal menu a discesa **Lingua prodotto** e fare clic su **Salva**. La modifica viene applicata dopo il successivo aggiornamento.

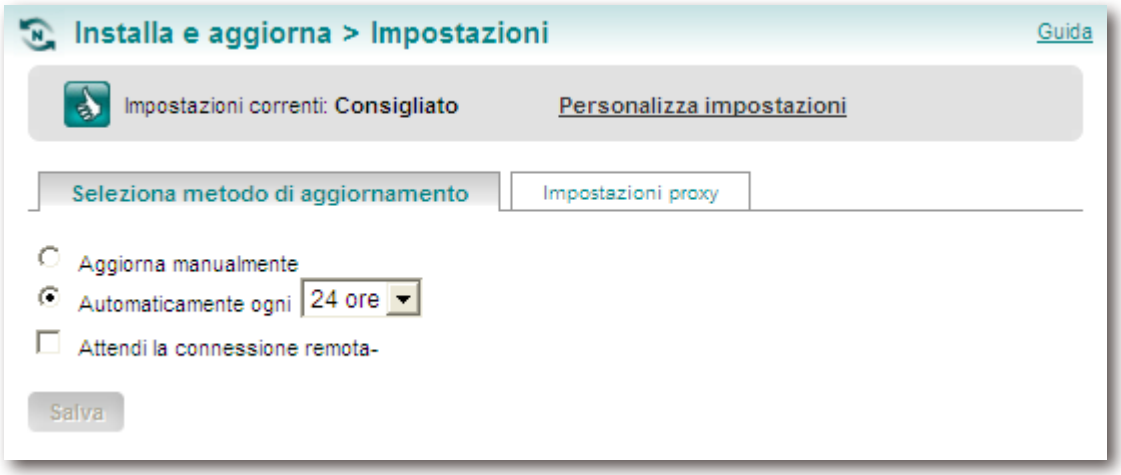
Gestione licenza guidata

La Gestione licenza guidata controlla e aggiorna le licenze. Se si seleziona questa opzione, viene visualizzata una finestra di dialogo con alcune informazioni sui prodotti installati e le credenziali delle chiavi di licenza. Per aggiornare l'installazione è necessaria una chiave valida.

Impostazioni

Seleziona metodo di aggiornamento

Questa opzione consente di scegliere tra l'aggiornamento manuale e automatico. Si consiglia il metodo automatico, perché è estremamente importante mantenere sempre aggiornato il software.



Copyright © 1990-2010 Norman ASA

Aggiorna manualmente

Selezionare questa opzione se si desidera eseguire manualmente l'Aggiornamento Internet dalla pagina principale Installa e aggiorna (Aggiorna tutti i prodotti). È anche possibile selezionare Aggiornamento Internet dal menu della barra delle applicazioni.

NOTA: l'opzione Aggiorna manualmente richiede un avvio forzato della funziona Aggiornamento Internet. Selezionando questa opzione, il sistema NON verrà aggiornato automaticamente. È altamente consigliato aggiornare il software frequentemente. L'aggiornamento manuale non è un metodo consigliato per l'uso quotidiano, perché è possibile dimenticarsi facilmente di eseguire l'aggiornamento.

Automaticamente a intervalli impostati

Selezionare questa opzione per rendere automatici il download e l'installazione degli aggiornamenti. Selezionare un intervallo di tempo nell'elenco accanto a **Automaticamente ogni** per impostare l'intervallo desiderato. Questa opzione richiede una connessione permanente a Internet.

NOTA: selezionando l'opzione per eseguire l'aggiornamento automaticamente a intervalli impostati, il sistema verrà aggiornato in modo automatico. Questa è l'opzione consigliata. Se non si esegue la funzionalità Aggiornamento Internet per 24 ore, il programma controlla automaticamente la disponibilità di nuovi aggiornamenti all'avvio.

Attendi la connessione remota

Se si utilizza un modem per la connessione a Internet, selezionare questa opzione per eseguire quotidianamente una ricerca degli aggiornamenti nei server dei prodotti. L'accesso a Internet avverrà come di consueto e il programma cercherà automaticamente i file di aggiornamento disponibili. Se ci si connette a Internet più volte al giorno, il meccanismo di aggiornamento verificherà l'eventuale presenza di aggiornamenti solo alla prima connessione. Se ci si connette a Internet una volta alla settimana, ad esempio, il programma eseguirà la verifica non appena stabilita la connessione.

Impostazioni proxy

Un server proxy è un computer che funge da intermediario tra il computer dell'utente e Internet. È possibile utilizzarlo per tenere traccia dell'utilizzo di Internet e per impedire l'accesso a determinati siti Web. Anche il firewall del server proxy può essere utilizzato per impedire l'accesso a determinati siti o pagine Web.

Se un firewall o un server proxy protegge il computer, occorre immettere le informazioni proxy richieste.

- Selezionare **Installa e aggiorna - Impostazioni - Impostazioni proxy**.
- Selezionare **Usa server proxy** e immettere un indirizzo proxy e una porta.
- Selezionare **Connetti al server proxy** e immettere nome utente, password e dominio (per Challenge/Response di Windows NT), se applicabile.
  - L'autenticazione basata sul meccanismo di richiesta/risposta (Challenge/Response) di Windows è il formato utilizzato per la connessione a Windows 2000 Server o a Windows Exchange.
  - L'account utente presenta il seguente formato: [*NT/2000nomedominio*]\[*nomeaccount*]

Copyright © 1990-2010 Norman ASA

Centro di supporto

Aprire l'applicazione Security Suite e selezionare **Centro di supporto** dal menu a sinistra. Fare riferimento alla sezione "Introduzione" a pagina 13 per informazioni su come aprire l'applicazione.

Pagina principale

Il **Centro di supporto** fornisce informazioni su come ottenere ulteriore assistenza oltre alle istruzioni disponibili nella documentazione del prodotto e nella Guida in linea. Contiene anche una funzione di riparazione automatica che può essere utile in caso di problemi con il software installato.

Guida e risoluzione dei problemi

Facendo clic sul collegamento **Guida e risoluzione dei problemi**, viene visualizzato il sito Web di Norman, che offre una gamma di utili risorse di supporto. Su questo sito Web sono disponibili:

- Supporto
- Security Center
- **Forum di supporto di Norman**

Se non è possibile risolvere il problema mediante queste risorse, contattare il rivenditore o la sede Norman locale.

Informazioni di contatto

Questa pagina contiene i numeri telefonici e gli indirizzi per contattare i rappresentanti Norman locali. Tali informazioni sono disponibili anche nell'ultima pagina del documento.

Copyright © 1990-2010 Norman ASA

Riparazione automatica

In caso di problemi con la versione di Security Suite installata, è possibile provare ad eseguire una riparazione automatica prima di contattare il personale del supporto.

Quando si fa clic su **Riparazione automatica**, viene avviato un processo in background che verifica l'installazione e, se necessario, aggiorna file o componenti. Viene visualizzato il simbolo di una ruota dentata nel menu della barra delle applicazioni durante la riparazione automatica. Vedere "Icone di avviso della barra delle applicazioni" a pagina 14 per una spiegazione delle icone relative a Security Suite.

Se non si dispone dell'accesso a un'interfaccia utente grafica, è possibile eseguire `delnvc5.exe` da `C:\Programmi\Norman\nvc\bin` e scegliere l'operazione **Ripara**.

Log dei messaggi

Questa è una funzione che controlla l'applicazione e visualizza diverse informazioni sui messaggi incluso tipo, autore, ora e data, applicazione e dettagli.

Copyright © 1990-2010 Norman ASA

Disinstallazione di NSS

Per disinstallare Norman Security Suite, sono disponibili due metodi. Mediante la funzione **Installazione applicazioni** di Windows oppure mediante l'applicazione di disinstallazione di Norman.

1. Dal sistema operativo Windows:
   - Selezionare **Start > Pannello di controllo > Installazione applicazioni**.
     - Su computer Vista selezionare **Programmi e funzionalità**.
   - Scorrere per individuare e selezionare l'applicazione Norman.
   - Selezionare l'opzione **Rimuovi**.
     - Una volta rimosso il programma, riavviare il computer.

2. Uso dell'applicazione di disinstallazione di Norman:
   - Selezionare **Start > Esegui** e immettere la posizione di `delnvc5.exe`
     - La posizione predefinita è `C:\Programmi\Norman\nvc\bin\delnvc5.exe`.
   - Selezionare l'opzione **Rimuovi**.
     - Quando richiesto, riavviare il computer.

Copyright © 1990-2010 Norman ASA

Appendice A

Sandbox

Sandbox è il termine che descrive meglio la tecnica utilizzata per controllare se un file è stato infettato da un virus sconosciuto. Il nome non è stato scelto a caso perché questo metodo consente di far "giocare" del codice, probabilmente infetto e considerato non attendibile, non nel computer vero bensì in un'area simulata e limitata al suo interno. Il "Sandbox" è dotato di tutto ciò che un virus si aspetta di trovare in un computer vero. In questa specie di parco giochi si consente al virus di replicarsi, ma al tempo stesso si controlla e si registra ogni suo passo. Il virus si espone e poiché le sue azioni vengono registrate è possibile generare automaticamente un rimedio.

Oggi un nuovo worm di posta elettronica può infettare decine di migliaia di workstation in pochi secondi. La funzionalità Sandbox di Norman può essere uno strumento prezioso per rilevare nuovo codice dannoso.

Copyright © 1990-2010 Norman ASA

Appendice B

Advanced System Reporter

Questo strumento è destinato agli utenti esperti. La sua funzionalità consente di rilevare spyware e rootkit sconosciuti ricercando eventuali anormalità nel computer. Le voci sospette come processi nascosti, processi ad auto-avvio sconosciuti, filtri di sistema sconosciuti, eccetera, possono rivelare applicazioni dannose.

NORMAN SecuritySuite
Advanced System Reporter
Livello di protezione: Protetto
Il computer sembra essere sicuro. Gli algoritmi di ricerca automatica in questo strumento non hanno rilevato alcuna voce sospetta. È possibile utilizzare comunque questo strumento per controllare manualmente le voci utilizzando le proprie conoscenze per rilevare le anomalie.
Processi nascosti rilevati: 0
DLL inserite non affidabili: 0
Filtri di rete non affidabili: 0
Altri filtri non affidabili: 0
Elementi interni del sistema operativo
Visualizza i filtri rilevati, le DLL inserite, i processi nascosti e i driver nonché le voci di registro sospette.
Vai alla vista
Internet Explorer
Controlla le impostazioni per Internet Explorer, visualizza i plugin rilevati e analizza i cookie.
Vai alla vista
Processi
Visualizza informazioni dettagliate sul processo.
Vai alla vista
Chiudi
Copyright (c) Norman ASA 1990-2010

Elementi interni del sistema operativo

Consente di visualizzare e modificare i dettagli per processi e driver nascosti, voci di registro, filtri installati e DLL inserite.

Selezione di Internet Explorer

Consente di visualizzare e modificare i dettagli per impostazioni, plugin e cookie.

Processi

Consente di visualizzare e modificare i dettagli dei processi per avvio automatico, servizi e altro.

Anche se l'utente esperto può considerare queste opzioni piuttosto semplici, facendo clic sul collegamento **Vai alla vista** nella parte inferiore della finestra Advanced System Reporter vengono fornite ulteriori informazioni su diversi argomenti.

Copyright © 1990-2010 Norman ASA

Elementi interni del sistema operativo

Processi nascosti

Un processo nascosto non è visibile in modalità utente, sebbene sia attualmente in esecuzione sul computer. Un processo nascosto in modalità utente è nascosto da un rootkit. Molto spesso si tratta di un driver che nasconde un processo in modalità utente dannoso rendendolo invisibile a un software antivirus standard.

Se si rilevano processi nascosti sul computer, è molto probabile che una o più voci sospette si trovino sotto la categoria Filtri installati. Queste voci sono il rootkit.

Voci di registro

Il registro viene interpretato in modo diverso in modalità utente e modalità kernel. Ciò significa che alcune tecniche nascondono voci di registro in applicazioni antivirus in modalità utente. Qualsiasi voce di registro che corrisponde a tali tecniche è considerata sospetta.

Filtri installati

Un filtro è un driver o una DLL che può connettersi a un'applicazione, che può modificare i dati prima che raggiungano un'applicazione.

- **LSP (Layered Service Provider)**
  Un LSP è un filtro di rete caricato in tutte le applicazioni quando caricano WinSock, il metodo comune utilizzato dalle applicazioni per accedere alla rete. Tali filtri di rete possono modificare e bloccare il traffico di rete in entrata e in uscita sul computer. Questa tecnologia è spesso utilizzata da prodotti Personal Firewall e Parental Control.
  Filtri di rete dannosi possono modificare i risultati della ricerca, spiare il traffico di rete, visualizzare messaggi pubblicitari indesiderati e reindirizzare a siti pericolosi.
- **SSDT (System Service Dispatch Table)**
  Questo driver speciale modifica la SSDT per filtrare operazioni eseguite da tutte le applicazioni, quali l'apertura o la lettura di un file oppure l'avvio di una nuova applicazione. Questa tecnica viene solitamente utilizzata da fornitori di software di sicurezza per impedire ad applicazioni pericolose d apportare modifiche dannose al computer.
  Tuttavia, un driver SSDT pericoloso può ottenere notevoli capacità di rootkit. Se si rileva un driver SSDT sconosciuto sul computer e uno o più processi nascosti, è molto probabile che sia presente un rootkit.

DLL inserite

Una DLL (Dynamic Link Library) è un modulo di programma memorizzato in un file separato per la condivisione tra diverse applicazioni o per l'estensione di applicazioni esistenti. Una DLL viene caricata dall'applicazione associata quando necessario.

- **DLL inserita**
  È possibile forzare un'applicazione in modo che carichi una DLL di una terza parte. Questa operazione viene effettuata anche se il fornitore dell'applicazione non l'aveva prevista e non carica esplicitamente la DLL. Tale tecnica è ampiamente utilizzata per malware, perché il modulo del codice all'interno della DLL può ottenere il controllo completo dell'applicazione. Può anche eseguire operazioni per conto dell'applicazione, mostrando al sistema operativo e al software per la sicurezza che l'operazione è stata eseguita dall'applicazione.
  Esistono alcune situazioni in cui è consentito inserire DLL in altre applicazioni. Ad esempio, per eseguire il debug di un'applicazione in caso di arresto anomalo. Solitamente, tuttavia, un'applicazione che inserisce DLL in altre applicazioni è progettata in modo scadente o pericoloso. Prestare particolare attenzione se si rilevano DLL inserite nel sistema. Qualsiasi DLL non proveniente da un fornitore affidabile deve essere eliminata. Anche il software scaricato e installato da Internet può essere un cavallo di troia.

Driver nascosti

Un driver nascosto non è visibile in modalità utente, sebbene sia attualmente in esecuzione sul computer. Un driver nascosto in modalità utente ha funzionalità di rootkit. Il driver nasconde i propri file sul disco rigido, le proprie voci di registro o il proprio spazio di memoria.

Copyright © 1990-2010 Norman ASA

Internet Explorer

Impostazioni
Consente di visualizzare e modificare le impostazioni per Microsoft Internet Explorer.

Plugin
Un plugin del browser offre funzioni aggiuntive come barre degli strumenti e miglioramenti delle funzionalità di ricerca, ma può anche offrire messaggi pubblicitari indesiderati e spiare abitudini di navigazione e password.

- **Oggetto browser helper**
  - Un oggetto browser helper (BHO) è un plugin di Internet Explorer che modifica il traffico in entrata e in uscita dal browser. Questo tipo di plugin è spesso utilizzato da applicazioni spyware, perché acquisisce facilmente tutti i dati inviati e ricevuti dal browser.
- **Barra degli strumenti**
  - Una barra degli strumenti è un plugin di Internet Explorer che crea nuove voci nel riquadro della barra degli strumenti del browser. Applicazioni adware utilizzano questo tipo di plugin per visualizzare messaggi pubblicitari.
- **Hook per la ricerca di URL**
  - Gli hook per la ricerca vengono utilizzati per reindirizzare gli indirizzi Web inseriti e possono essere di ausilio nella risoluzione di indirizzi errati o incompleti. Ad esempio, norman.com verrà convertito automaticamente in http://www.norman.com. Le applicazioni adware utilizzano questo tipo di plugin per reindirizzare l'utente ad altri siti Web.
- **Altro**
  - Altri plugin possono aggiungere opzioni di menu o pannelli utente al browser Applicazioni adware utilizzano questo tipo di plug-in per visualizzare messaggi pubblicitari.

NOTA: tecnicamente, tutti i plugin possono modificare traffico e spiare i dati degli utenti, anche se il plugin specifico non è destinato a tale scopo.

Cookie
Un cookie è un piccolo file che viene memorizzato tra i file temporanei di Internet in seguito alla visualizzazione di una pagina Web.

- **Convinzione errata**
  - È una tipica convinzione errata che i cookie siano dannosi, che generano popup e pubblicità indesiderate e che possono danneggiare il computer. Effettivamente alcuni fornitori di prodotti antispyware li elencano come spyware e generano anche allarmi per alcuni cookie. Specialmente nel caso dei cosiddetti 'cookie di traccia'.
  - I cookie NON SONO PERICOLOSI e non possono danneggiare il computer. I cookie visualizzati in questa finestra di dialogo non rappresentano una minaccia. Tuttaiva, è possibile comunque rimuoverli.
- **Uso dei cookie**
  - I cookie vengono utilizzati dai server Web per effettuare una differenziazione tra gli utenti e per tenere traccia dello stato. Se si elimina un cookie si perdono preferenze utente, carrelli e le credenziali di accesso, anche da un accesso all'altro. In questo caso, ad esempio, sarà necessario eseguire nuovamente il login.
- **Cookie di traccia**
  - Alcuni siti Web utilizzano cookie di terze parti per tenere traccia degli spostamenti dell'utente tra i vari siti. Alcuni ritengono che sia un'invasione della privacy, ma i server Web visitati possono trasferire tali informazioni direttamente tra di loro senza dover necessariamente affidarsi ai cookie di traccia.
  - Questo strumento non effettua una distinzione tra i "cookie di traccia" e i "cookie normali" poiché l'unica differenza consiste nel fatto che il cookie è gestito da terze parti. Nessuno dei due è potenzialmente più pericoloso dell'altro.

Copyright © 1990-2010 Norman ASA

Processi

Avvio automatico

Se un'applicazione, legittima o dannosa, viene installata sul computer, molto probabilmente verrà avviata automaticamente a ogni avvio del computer. Un programma che prevede l'avvio automatico può indicare al sistema operativo di auto-avviarsi con gli stessi privilegi dell'utente corrente oppure installare un servizio di background che viene eseguito con privilegi superiori. Questa applicazione è in grado di interrompere tali tentativi.

NOTA: la funzione di avvio automatico non riguarda la funzione di esecuzione automatica per CD o dispositivi USB.

Servizi

Un servizio è un processo di background avviato ogni volta che si avvia il computer. Questo è il funzionamento standard.

Copyright © 1990-2010 Norman ASA

Sedi Norman

Danmark
Norman Data Defense Systems AS
Blangstedgårdsvej 1,
DK-5220 Odense SØ
Tel: +45 63 11 05 08
Fax: +45 65 90 51 02
E-mail: info@normandk.com
Web: www.norman.com/dk

Deutschland
Norman Data Defense Systems GmbH
Zentrale, Gladbecker Str. 3,
D-40472 Düsseldorf
Tel: +49 0211 5 86 99-0
Fax: +49 0211 5 86 99-150
E-mail: info@norman.de
Web: www.norman.com/de

España
Norman Data Defense Systems
Camino Cerro de los Gamos 1, Edif.1,
28224 Pozuelo de Alarcón MADRID
Tel: +34 91 790 11 31
Fax: +34 91 790 11 12
E-mail: norman@normandata.es
Web: www.norman.com/es

France
Norman France
8 Rue de Berri,
F-75008 Paris
Tel: +33 1 42 99 94 14
Fax: +33 1 42 99 95 01
E-mail: info@norman.fr
Web: www.norman.com/fr

Italia
Norman Data Defense Systems
Centro Cassina Plaza,
Via Roma, 108
20060 Cassina de'Pecchi (MI)
Tel: +39 02 951 58 952
Fax: +39 02 951 38 270
E-mail: info@normanit.com
Web: www.norman.com/it

Nederland
Norman SHARK B.V.
Postbus 159,
2130 AD Hoofddorp
Tel: +31 23 789 02 22
Fax: +31 23 561 31 65
E-mail: support@norman.nl
Web: www.norman.com/nl

Norge
Norman ASA
Headquarter and sales Norway
Hovedkontor og salg Norge
Visit: Strandveien 37, Lysaker
Mail: PO Box 43, N-1324 Lysaker
Tel: +47 67 10 97 00
Fax: +47 67 58 99 40
E-mail: norman@norman.no
Web: www.norman.com/no

Schweiz/Suisse/Svizzera
Norman Data Defense Systems AG
Münchensteinerstrasse 43
CH-4052 Basel
Tel: +41 61 317 25 25
Fax: +41 61 317 25 26
E-mail: norman@norman.ch
Web: www.norman.com/ch

Sverige
Norman Data Defense Systems AB
Södra Grytsgatan 7, 2tr,
Norrköping Science Park
S-602 33 Norrköping
Tel: +46 11 230 330
Fax: +46 11 230 349
E-mail: sales.se@norman.com
Web: www.norman.com/se

United Kingdom
Norman Data Defense Systems (UK) Ltd
Exchange House,
494 Midsummer Boulevard
Central Milton Keynes,
MK9 2EA
Tel1: +44 08 707 448 044
Tel2: +44 01 908 255 990
Fax: +44 08 701 202 901
E-mail: info@normanuk.com
Web: www.norman.com/en-uk

United States
Norman Data Defense Systems Inc.
9302 Lee Highway,
Suite 950A,
Fairfax, Virginia 22031
Tel: +1 703 267 6109
Fax: +1 703 934 6368
E-mail: norman@norman.com
Web: www.norman.com/en-us

Norman ASA è una società leader in tutto il mondo nel campo della sicurezza dei dati, della protezione Internet e degli strumenti di analisi. Mediante la tecnologia Sandbox Norman offre una protezione unica e proattiva rispetto a qualsiasi altra azienda concorrente. Pur concentrandosi sulla sua tecnologia antivirus proattiva, la società ha costituito diverse alleanze che consentono a Norman di offrire una gamma completa di servizi per la sicurezza dei dati.

Norman è stata fondata nel 1984, la sede principale è in Norvegia e i principali mercati sono Europa, Regno Unito e Stati Uniti.

Copyright © 1990-2010 Norman ASA

NORMAN®